

Reference

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2003 年 6 月 5 日 (05.06.2003)

PCT

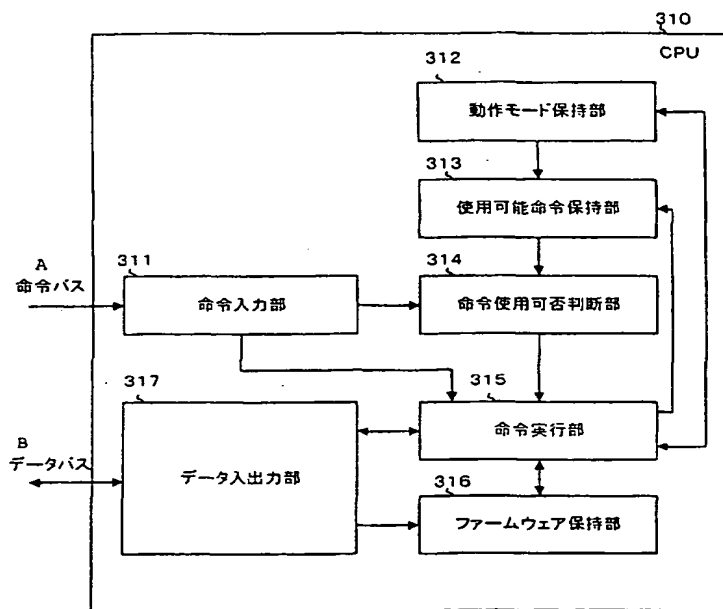
(10) 国際公開番号
WO 03/046715 A1

- (51) 国際特許分類⁷: G06F 9/30, 9/06 (72) 発明者: および
(21) 国際出願番号: PCT/JP01/10446 (75) 発明者/出願人 (米国についてのみ): 蒲田 順
(22) 国際出願日: 2001 年 11 月 29 日 (29.11.2001) (KAMADA, Jun) [JP/JP]. 小谷 誠剛 (KOTANI, Seigo)
(25) 国際出願の言語: 日本語 [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中 4
(26) 国際公開の言語: 日本語 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP).
(74) 代理人: 酒井 宏明 (SAKAI, Hiroaki); 〒100-0013 東京
都千代田区霞ヶ関三丁目 2 番 6 号 東京倶楽部ビルディ
ング Tokyo (JP).
(71) 出願人 (米国を除く全ての指定国について): 富士通
株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神
奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 Kanagawa
(JP). (81) 指定国 (国内): JP, US.
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[続葉有]

(54) Title: CENTRAL PROCESSING DEVICE AND OPERATION PROGRAM

(54) 発明の名称: 中央演算装置および演算プログラム



(57) Abstract: A central processing device comprises an operating mode holding unit (312) holding one or more of a plurality of operating modes, an available instruction holding unit (313) holding an instruction corresponding to the operating mode held by the operating mode holding unit (312) as an available instruction, and an instruction executing unit (315) for adding a dynamically designated operating modes out of the operating modes to the operating mode holding unit (312), for setting an instruction corresponding to the added operating mode in the available instruction holding unit (313), and for acquiring firmware corresponding to the operating mode held in the operating mode holding unit (312) and used for executing the instruction from the outside.

A...INSTRUCTION BUS
B...DATA BUS
311...INSTRUCTION INPUT UNIT
317...DATA INPUT/OUTPUT UNIT
312...OPERATING MODE HOLDING UNIT
313...AVAILABLE INSTRUCTION HOLDING UNIT
314...INSTRUCTION AVAILABILITY JUDGING UNIT
315...INSTRUCTION EXECUTION UNIT
316...FIRMWARE HOLDING UNIT

[続葉有]

WO 03/046715 A1



添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

複数の動作モードのうち単数または複数の動作モードを保持する動作モード保持部 3 1 2 と、動作モード保持部 3 1 2 により保持された動作モードに対応する命令を、使用可能命令として保持する使用可能命令保持部 3 1 3 と、複数の動作モードのうち動的に指定された動作モードを動作モード保持部 3 1 2 に追加し、追加された動作モードに対応する命令を使用可能命令保持部 3 1 3 に設定し、さらに動作モード保持部 3 1 2 に保持された動作モードに対応し、命令の実行に用いられるファームウェアを外部から取得する命令実行部 3 1 5 とを備えている。

明 細 書

中央演算装置および演算プログラム

5 技術分野

本発明は、例えば、セキュリティ機能を実現するための中央演算装置および演算プログラムに関するものであり、特に、セキュリティを維持しつつ、拡張性を高めることができる中央演算装置および演算プログラムに関するものである。

10 背景技術

近年、インターネット上での電子商取引が活発化するに従って、より高度なセキュリティが求められている。従って、電子商取引に用いられる計算機には、認証、暗号化／復号、電子署名生成／検証等の各セキュリティ機能が不可欠となる。理想的には、各セキュリティ機能が独立した複数の計算機からなるセキュリティシステムにより実現されることが望ましい。

第46図は、上述した従来のセキュリティシステムの構成を示すブロック図である。この図において、計算機10は、インターネット20およびイントラネット30に接続されており、上述したセキュリティ機能としての認証を認証用CPU (Central Processing Unit: 中央演算装置) 11により実現するためのものである。この認証用CPU 11は、セキュリティを高めるため、認証用の命令群のみを利用可能に構成されている。

計算機40は、イントラネット30に接続されており、セキュリティ機能としての暗号化／復号を暗号化／復号用CPU 41により実現するためのものである。この暗号化／復号用CPU 41も、セキュリティを高めるため、暗号化／復号固有の命令群のみを利用可能に構成されている。

計算機50は、イントラネット30に接続されており、セキュリティ機能としての電子署名生成／検証を電子署名生成／検証用CPU 51により実現するため

のものである。この電子署名生成／検証用CPU51も、セキュリティを高めるため、電子署名生成／検証固有の命令群のみを利用可能に構成されている。

計算機60は、イントラネット30に接続されており、セキュリティ機能以外の一般機能を一般用CPU61により実現するためのものである。一般用CPU
5 61は、一般固有の命令群のみを利用可能に構成されている。このように、従来のセキュリティシステムは、各計算機でセキュリティ機能を実現している。

ところで、前述した従来のセキュリティシステムにおいては、セキュリティを高める目的で各計算機で使用可能な命令群が固定的に設定されているため、拡張性に乏しいという問題があった。

10 特に、セキュリティ技術の進歩が目覚ましい昨今においては、最新のセキュリティ技術が出現する毎に、新規の命令群を組み込んだ計算機にリプレースする必要があるため、コストが高くつくという問題も発生する。

本発明は、上記に鑑みてなされたもので、セキュリティを維持しつつ拡張性を高めることができ、コストを低減させることができる中央演算装置および演算プ
15 ログラムを提供することを目的としている。

発明の開示

上記目的を達成するために、本発明は、複数の動作モードのうち単数または複数の動作モードを保持する動作モード保持手段と、前記動作モード保持手段により保持された動作モードに対応する命令を、使用可能命令として保持する使用可能命令保持手段と、前記複数の動作モードのうち動的に指定された動作モードを前記動作モード保持手段に追加し、追加された動作モードに対応する命令を前記使用可能命令保持手段に設定する動作モード追加手段と、前記動作モード保持手段に保持された動作モードに対応し、命令の実行に用いられるファームウェアを
20 外部から取得するファームウェア取得手段とを備えたことを特徴とする。

また、本発明は、コンピュータを、複数の動作モードのうち単数または複数の動作モードを保持する動作モード保持手段、前記動作モード保持手段により保持

された動作モードに対応する命令を、使用可能命令として保持する使用可能命令保持手段、前記複数の動作モードのうち動的に指定された動作モードを前記動作モード保持手段に追加し、追加された動作モードに対応する命令を前記使用可能命令保持手段に設定する動作モード追加手段、前記動作モード保持手段に保持された動作モードに対応し、命令の実行に用いられるファームウェアを外部から取得するファームウェア取得手段として機能させるための演算プログラムである。

かかる発明によれば、複数の動作モードのうち動的に指定された動作モードを動作モード保持手段に追加し、追加された動作モードに対応する命令を使用可能命令保持手段に設定し、さらに、命令の実行に用いられるファームウェアを外部から取得するようにしたので、セキュリティを維持しつつ拡張性を高めることができ、コストを低減させることができる。

また、本発明は、複数の動作モードのうち単数または複数の動作モードを保持する動作モード保持手段と、前記動作モード保持手段により保持された動作モードに対応する命令を、使用可能命令として保持する使用可能命令保持手段と、前記複数の動作モードのうち動的に指定された動作モードを前記動作モード保持手段に追加し、追加された動作モードに対応する命令を前記使用可能命令保持手段に設定する動作モード追加手段と、前記動作モード保持手段に保持された動作モードに対応し、命令の実行に用いられる論理回路を生成するための論理回路データを外部から取得する論理回路データ取得手段とを備えたことを特徴とする。

この発明によれば、複数の動作モードのうち動的に指定された動作モードを動作モード保持手段に追加し、追加された動作モードに対応する命令を使用可能命令保持手段に設定し、さらに、動作モード保持手段に保持された動作モードに対応し、命令の実行に用いられる論理回路を生成するための論理回路データを外部から取得するようにしたので、セキュリティを維持しつつ拡張性を高めることができ、コストを低減させることができる。

第1図は、本発明にかかる実施の形態1の構成を示すブロック図であり、第2図は、第1図に示したCPU310の構成を示すブロック図であり、第3図は、同実施の形態1における動作モード/命令対応表400を示す図であり、第4図は、第2図に示したCPU310、第27図に示したCPU1110、第34図に示したCPU310および第43図に示したCPU1510の動作を説明するフローチャートであり、第5図は、第4図、第18図および第23図に示した通常命令実行処理を説明するフローチャートであり、第6図は、第4図、第18図および第23図に示した動作モード追加処理を説明するフローチャートであり、第7図は、第4図に示したファームウェアダウンロード処理を説明するフローチャートであり、第8図は、同実施の形態1の動作を説明するフローチャートであり、第9図は、本発明にかかる実施の形態2の構成を示すブロック図であり、第10図は、第9図に示したCPU610の構成を示すブロック図であり、第11図は、第10図に示したCPU610の動作を説明するフローチャートであり、第12図は、第11図に示した通常命令実行処理を説明するフローチャートであり、第13図は、第11図に示した動作モード追加処理を説明するフローチャートであり、第14図は、第11図に示した論理回路データダウンロード処理を説明するフローチャートであり、第15図は、同実施の形態2の動作を説明するフローチャートであり、第16図は、本発明にかかる実施の形態3の構成を示すブロック図であり、第17図は、第16図に示したCPU810の構成を示すブロック図であり、第18図は、第17図に示したCPU810の動作を説明するフローチャートであり、第19図は、第18図に示した暗号化ファームウェアダウンロード処理を説明するフローチャートであり、第20図は、同実施の形態3の動作を説明するフローチャートであり、第21図は、本発明にかかる実施の形態4の構成を示すブロック図であり、第22図は、第21図に示したCPU1010の構成を示すブロック図であり、第23図は、第21図に示したCPU1010の動作を説明するフローチャートであり、第24図は、第23図に示した電子署名付きファームウェアダウンロード処理を説明するフローチャートであり、

第25図は、同実施の形態4の動作を説明するフローチャートであり、第26図は、本発明にかかる実施の形態5の構成を示すブロック図であり、第27図は、第26図に示したCPU1110の構成を示すブロック図であり、第28図は、同実施の形態5における動作モード／資源対応表1200を示す図であり、第29図は、同実施の形態5における通常命令実行処理を説明するフローチャートであり、第30図は、第29図に示したアクセス制御処理を説明するフローチャートであり、第31図は、同実施の形態5における動作モード追加処理を説明するフローチャートであり、第32図は、本発明にかかる実施の形態6の構成を示すブロック図であり、第33図は、同実施の形態6における動作モードファイル1321。～1321。のデータ構造を示す図であり、第34図は、第32図に示したオペレーティングシステム1310およびCPU310の構成を示すブロック図であり、第35図は、第34図に示したオペレーティングシステム1310の動作を説明するフローチャートであり、第36図は、本発明にかかる実施の形態7の構成を示すブロック図であり、第37図は、第36図に示したCPU1410およびオペレーティングシステム1420の構成を示すブロック図であり、第38図は、第37図に示したCPU1410の動作を説明するフローチャートであり、第39図は、第38図に示した動作モード削除処理を説明するフローチャートであり、第40図は、第38図に示したファームウェアアンロード処理を説明するフローチャートであり、第41図は、第37図に示したオペレーティングシステム1420の動作を説明するフローチャートであり、第42図は、本発明にかかる実施の形態8の構成を示すブロック図であり、第43図は、第42図に示したCPU1510およびエミュレート部1520の構成を示すブロック図であり、第44図は、第43図に示したエミュレート部1520の動作を説明するフローチャートであり、第45図は、本発明にかかる実施の形態1～8の変形例の構成を示すブロック図であり、第46図は、従来のセキュリティシステムの構成を示すブロック図である。

発明を実施するための最良の形態

以下、図面を参照して本発明にかかる実施の形態 1 ～ 8 について詳細に説明する。

(実施の形態 1)

- 5 第 1 図は、本発明にかかる実施の形態 1 の構成を示すブロック図である。この図において、サーバ 100 は、各種ファームウェアをクライアント 300 へインターネット 200 を介して提供する。サーバ 100 において、CPU 110 は、ファームウェア提供に関する制御を行う。

- メモリ 120 は、CPU 110 での制御に関する各種データを保持するものであり、例えば、RAM (Random Access Memory) や ROM (Read Only Memory) 10 等である。ファームウェア格納部 130 は、後述する CPU 310 での命令実行に用いられるファームウェアを複数格納している。これらのファームウェアは、ファームウェア番号に対応付けられて、ファームウェア格納部 130 に格納されている。

- 15 通信部 140 は、TCP/IP (Transmission Control Protocol/Internet Protocol) 等の通信プロトコルにしたがって、サーバ 100 での通信制御を行う。

- クライアント 300 は、インターネット 200 に接続されており、インターネット 200 を介して、サーバ 100 からファームウェアをダウンロードする機能と、ファームウェアを用いて各種命令を実行し、結果を出力する機能とを備えて 20 いる。

- クライアント 300 において、CPU 310 は、ファームウェアを動的にダウンロードさせるための制御や、後述する動作モードや命令群の設定等を行う。メモリ 320 は、CPU 310 での制御に関する各種データを保持するものであり、例えば、RAM や ROM 等である。ダウンロード部 330 は、CPU 310 の制 25 御により、サーバ 100 からファームウェアをダウンロードする。入力部 350 は、キーボード、マウス等の入力デバイスである。表示部 360 は、CPU 310 での命令の実行結果等を表示するディスプレイである。

第2図は、第1図に示したCPU 310の構成を示すブロック図である。この図において、命令入力部311は、命令バスを介して命令を入力し、これを命令実行部315および命令使用可否判断部314にフェッチする。動作モード保持部312は、CPU 310の動作モードを保持する。

5 第3図には、上記動作モードと命令との対応関係を表す動作モード／命令対応表400が図示されている。この動作モード／命令対応表400において、動作モードは、「0」～「k」とされている。使用可能命令数は、動作モード毎に設定されており、当該動作モード時に命令実行部315で使用可能な命令の数である。

10 例えば、動作モード=0の場合には、使用可能命令数がnである。すなわち、動作モード0の場合には、命令1(0x01)～命令n(0xf8)という都合n種類の命令が命令実行部315で使用可能である。

また、動作モード=1の場合には、使用可能命令数がiである。すなわち、動作モード1の場合には、命令1(0x11)～命令i(0xe7)という都合i
15 種類の命令が命令実行部315で使用可能である。また、動作モード=1のみが設定されている場合、命令実行部315では、命令1(0x11)～命令i(0xe7)以外の命令が使用できない。

同様に、動作モード=kの場合には、使用可能命令数が1である。すなわち、動作モードkの場合には、命令1(0xff)という都合1種類の命令が命令
20 実行部315で使用可能である。また、動作モード=kのみが設定されている場合、命令実行部315では、命令1(0xff)以外の命令が使用できない。
また、動作モード保持部312に設定される動作モードは、動的に追加される。

第2図に戻り、使用可能命令保持部313は、動作モード保持部312に設定された動作モードに対応する使用可能命令を保持する。

25 例えば、第3図に示した動作モード=0が動作モード保持部312に設定されている場合、使用可能命令保持部313には、動作モード=0に対応する命令1(0x01)～命令n(0xf8)が使用可能命令として保持される。

命令使用可否判断部 3 1 4 は、命令入力部 3 1 1 にフェッチされた命令が、使用可能であるか否かを判断する。具体的には、命令使用可否判断部 3 1 4 は、フェッチされた当該命令が、動作モード／命令対応表 4 0 0（第 3 図参照）を参照して、動作モード保持部 3 1 2 に設定されている現在の動作モードで使用可能な命令群に含まれている場合、使用可能と判断する。

一方、フェッチされた命令が当該命令群に含まれていない場合、使用不可と判断する。このように、実施の形態 1 では、動作モードに応じて使用可能な命令を制限している。

命令実行部 3 1 5 は、命令使用可否判断部 3 1 4 により使用可能と判断された命令を実行する。また、命令実行部 3 1 5 は、当該命令の実行に用いられるファームウェアをファームウェア保持部 3 1 6 より取得する。

ファームウェア保持部 3 1 6 は、動作モード保持部 3 1 2 に設定された動作モードでの命令群に対応するファームウェアを保持する。このファームウェアは、サーバ 1 0 0（第 1 図参照）からダウンロードされたものである。また、動作モードが追加されたことにより新規命令が追加された場合、ファームウェア保持部 3 1 6 には、新規のファームウェアが保持される。

データ入出力部 3 1 7 は、データバスを介して、命令実行部 3 1 5 での命令の実行に必要な各種データを入力する機能と、実行結果を出力する機能とを備えている。

つぎに、実施の形態 1 の動作について、第 4 図～第 8 図に示したフローチャートを参照しつつ説明する。第 4 図に示したステップ S A 1 では、CPU 3 1 0 は、通常命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。通常命令は、後述する動作モード追加命令およびファームウェアダウンロード命令以外の命令であって、CPU 3 1 0 で実行される命令である。

ステップ S A 2 では、CPU 3 1 0 は、動作モード追加命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。動作モード追加命令は、第 3 図に示した動作モード／命令対応表 4 0 0 の動作モードを追加するための命令

である。

ステップSA3では、CPU310は、ファームウェアダウンロード命令が入力されたか否かを判断し、この場合、判断結果を「No」とし、ステップSA1の判断を行う。ファームウェアダウンロード命令は、インターネット200を介して、サーバ100から取得したファームウェアをCPU310内に設定するための命令である。以後、CPU310は、ステップSA1～ステップSA3の判断を繰り返す。

そして、通常命令が入力されると、CPU310は、ステップSA1の判断結果を「Yes」とする。ステップSA4では、CPU310は、通常命令実行処理を実行する。

具体的には、第5図に示したステップSB1では、命令入力部311（第2図参照）は、命令バスを介して入力された通常命令を命令使用可否判断部314および命令実行部315にフェッチする。ステップSB2では、動作モード保持部312は、現時点で設定されている動作モードを使用可能命令保持部313へ通知する。ここで通知された動作モードは、第3図に示した「1」とする。

ステップSB3では、使用可能命令保持部313は、通知された動作モードに対応する命令群を使用可能命令群として命令使用可否判断部314へ通知する。この場合の使用可能命令群は、第3図に示した動作モード＝1に対応する命令1（0x11）～命令i（0xe7）である。

ステップSB4では、命令使用可否判断部314は、ステップSB1でフェッチされた通常命令が、当該動作モードで使用可能であるか否かを判断する。具体的には、命令使用可否判断部314は、ステップSB3で通知された使用可能命令群に、ステップSB1でフェッチされた通常命令が存在するか否かを判断し、この場合、判断結果を「Yes」とする。

ステップSB5では、命令実行部315は、ステップSB1でフェッチされた通常命令（使用可能命令）に対応するファームウェアをファームウェア保持部316から取得する。ステップSB6では、命令実行部315は、データ入出力部

3 1 7 より、命令実行に用いられるデータを取得する。ステップ S B 7 では、命令実行部 3 1 5 は、ファームウェアおよびデータを用いて通常命令を実行する。ステップ S B 8 では、命令実行部 3 1 5 は、通常命令を実行した結果をデータ入出力部 3 1 7 を経由して出力する。

- 5 一方、ステップ S B 4 の判断結果が「N o」である場合、すなわち、ステップ S B 1 でフェッチされた通常命令が当該動作モード＝1 で使用不可である場合、ステップ S B 9 では、命令使用可否判断部 3 1 4 は、権限違反または未定義命令例外割り込み発生（エラー）として処理する。

- 10 ここで、CPU 3 1 0 において、第 3 図に示した動作モード＝1 の命令群に含まれない命令 n (0 x f 8) (動作モード＝0) を実行できるようにする場合には、動作モード＝1 を追加すればよい。以下では、動作モード追加処理について説明する。

- 動作モード追加命令が入力されると、CPU 3 1 0 は、第 4 図に示したステップ S A 2 の判断結果を「Y e s」とする。ステップ S A 5 では、CPU 3 1 0 は、
15 動作モード追加処理を実行する。

- 具体的には、第 6 図に示したステップ S C 1 では、命令入力部 3 1 1 (第 2 図参照) は、命令バスを介して入力された動作モード追加命令を命令使用可否判断部 3 1 4 および命令実行部 3 1 5 にフェッチする。ステップ S C 2 では、動作モード保持部 3 1 2 は、現時点で設定されている動作モード（この場合、動作モード＝1) を使用可能命令保持部 3 1 3 へ通知する。
20

ステップ S C 3 では、使用可能命令保持部 3 1 3 は、通知された動作モード＝1 に対応する命令 1 (0 x 1 1) ～命令 i (0 x e 7) を使用可能命令群として命令使用可否判断部 3 1 4 へ通知する。

- ステップ S C 4 では、命令使用可否判断部 3 1 4 は、ステップ S C 1 でフェッチされた動作モード追加命令が、当該動作モードで使用可能であるか否かを判断する。具体的には、命令使用可否判断部 3 1 4 は、ステップ S C 3 で通知された使用可能命令群に、ステップ S C 1 でフェッチされた動作モード追加命令が存在
25

するか否かを判断し、この場合、判断結果を「Y e s」とする。

ステップS C 5では、命令実行部3 1 5は、ステップS C 1でフェッチされた動作モード追加命令（使用可能命令）に対応するファームウェアをファームウェア保持部3 1 6から取得する。

5 ステップS C 6では、命令実行部3 1 5は、データ入出力部3 1 7より、動作モードデータおよび命令群を取得する。この場合、動作モードデータは、追加すべき動作モードに対応する「0」（第3図参照）である。また、命令群は、第3図に示した動作モード=0に対応する命令1（0 x 0 1）～命令n（0 x f 8）である。

10 ステップS C 7では、命令実行部3 1 5は、動作モード保持部3 1 2に追加する動作モード=0を設定するとともに、使用可能命令保持部3 1 3に動作モード=0に対応する命令群を設定する。これにより、動作モード=0での命令群が使用可能となる。

15 一方、ステップS C 4の判断結果が「N o」である場合、すなわち、ステップS C 1でフェッチされた動作モード追加命令が当該動作モード=1で使用不可である場合、ステップS C 8では、命令使用可否判断部3 1 4は、権限違反または未定義命令例外割り込み発生（エラー）として処理する。

20 ここで、上述した動作モード追加処理により追加された動作モード=0に対応する命令群において、命令実行時に必要なファームウェアがファームウェア保持部3 1 6に保持されていない場合、当該ファームウェアをサーバ1 0 0からダウンロードする必要がある。以下では、ファームウェアダウンロード処理について説明する。

25 この場合、第8図に示したステップS E 1では、第1図に示したダウンロード部3 3 0は、C P U 3 1 0よりダウンロード要求があるか否かを判断し、この場合、判断結果を「N o」として同判断を繰り返す。

そして、C P U 3 1 0からダウンロード部3 3 0へ、当該ファームウェアをダウンロードする要求があると、ダウンロード部3 3 0は、ステップS E 1の判断

結果を「Y e s」とする。ステップS E 2では、ダウンロード部330は、ファームウェア／ファームウェア番号対応表（図示略）に基づいて、CPU310から要求されたファームウェアに対応するファームウェア番号を指定する。つぎに、ダウンロード部330は、当該ファームウェア番号に基づいて、インターネット
5 200を介してサーバ100へファームウェアダウンロード要求を出す。

これにより、ステップS E 3では、サーバ100のCPU110は、ファームウェア番号をキーとして、ファームウェア格納部130から当該ファームウェアを読み出し、これをクライアント300のダウンロード部330へ転送する。

当該ファームウェアが転送されると、ステップS E 4では、ダウンロード部3
10 30は、CPU310に対して、ファームウェアダウンロード命令を発行した後、ステップS E 1の判断を行う。

そして、上記ファームウェアダウンロード命令が入力されると、CPU310は、第4図に示したステップS A 3の判断結果を「Y e s」とする。ステップS A 6では、CPU310は、ファームウェアダウンロード処理を実行する。

15 具体的には、第7図に示したステップS D 1では、命令入力部311（第2図参照）は、命令バスを介して入力されたファームウェアダウンロード命令を命令使用可否判断部314および命令実行部315にフェッチする。ステップS D 2では、動作モード保持部312は、現時点で設定されている動作モード（この場合、動作モード＝0、1）を使用可能命令保持部313へ通知する。

20 ステップS D 3では、使用可能命令保持部313は、通知された動作モード＝0、1に対応する命令1（0 x 0 1）～命令n（0 x f 8）、命令1（0 x 1 1）～命令i（0 x e 7）を使用可能命令群として命令使用可否判断部314へ通知する。

ステップS D 4では、命令使用可否判断部314は、ステップS D 1でフェッ
25 チされたファームウェアダウンロード命令が、当該動作モード0、1で使用可能であるか否かを判断する。具体的には、命令使用可否判断部314は、ステップS D 3で通知された使用可能命令群に、ステップS D 1でフェッチされたファームウェアダウンロード命令が、当該動作モード0、1で使用可能であるか否かを判断する。

ムウェアダウンロード命令が存在するか否かを判断し、この場合、判断結果を「Yes」とする。

ステップSD 5では、命令実行部315は、ステップSD 1でフェッチされたファームウェアダウンロード命令（使用可能命令）に対応する実行用のファームウェアをファームウェア保持部316から取得する。

ステップSD 6では、命令実行部315は、ファームウェアダウンロード命令およびこれに対応する実行用のファームウェアに基づいて、データ入出力部317およびデータバスを介してダウンロード部330から設定用のファームウェアを取得する。

10 ステップSD 7では、命令実行部315は、設定用のファームウェアをファームウェア保持部316に設定する。これにより、前述した動作モード追加処理により追加された動作モード=0での命令群が使用可能となる。

一方、ステップSD 4の判断結果が「No」である場合、すなわち、ステップSD 1でフェッチされたファームウェアダウンロード命令が当該動作モード=0、
15 1で使用不可である場合、ステップSD 8では、命令使用可否判断部314は、権限違反または未定義命令例外割り込み発生（エラー）として処理する。

以上説明したように、実施の形態1によれば、複数の動作モードのうち動的に指定された動作モードを第2図に示した動作モード保持部312に追加し、追加された動作モードに対応する命令を使用可能命令保持部313に設定し、さらに、
20 命令の実行に用いられるファームウェアを外部のサーバ100（第1図参照）から取得するようにしたので、セキュリティを維持しつつ拡張性を高めることができ、コストを低減させることができる。

（実施の形態2）

さて、前述した実施の形態1では、命令実行部315（第2図参照）でファームウェアを用いて命令を実行する例について説明したが、ファームウェアに代えて論理回路を用いて命令を実行する構成としてもよい。以下では、この構成例を実施の形態2として説明する。

第9図は、本発明にかかる実施の形態2の構成を示すブロック図である。この図において、第1図の各部に対応する部分には同一の符号を付け、その説明を省略する。サーバ500は、論理回路データをクライアント600へインターネット200を介して提供する。

- 5 論理回路データは、実施の形態1におけるファームウェアの機能を実現するための論理回路を生成するためのデータである。サーバ500において、CPU510は、論理回路データ提供に関する制御を行う。

- 論理回路データ格納部520は、後述するCPU610での命令実行に用いられる論理回路を生成するための論理回路データを複数格納している。これらの論理回路データは、論理回路データ番号に対応付けられて、論理回路データ格納部
10 520に格納されている。

- クライアント600は、インターネット200に接続されており、インターネット200を介して、サーバ500から論理回路データをダウンロードする機能と、論理回路データより論理回路を生成する機能と、該論理回路を用いて各種命令を実行し、結果を出力する機能とを備えている。
15

クライアント600において、CPU610は、論理回路データを動的にダウンロードさせるための制御や、後述する動作モードや命令群の設定等を行う。ダウンロード部620は、CPU610の制御により、サーバ500から論理回路データをダウンロードする。

- 20 第10図は、第9図に示したCPU610の構成を示すブロック図である。この図において、第2図の各部に対応する部分には同一の符号を付け、その説明を省略する。CPU610において、命令実行部611は、動的に生成される論理回路を備えており、命令使用可否判断部314により使用可能と判断された命令を論理回路により実行する。また、命令実行部611は、当該命令に対応する論理回路データに基づいて、論理回路生成部612に論理回路を動的に生成させる。
25 論理回路生成部612は、動作モード保持部312に設定された動作モードでの命令群に対応する論理回路データを保持しており、命令実行部611の制御の下

で、命令実行部 6 1 1 で実行すべき命令に対応する論理回路を命令実行部 6 1 1 内に生成する。

つぎに、実施の形態 2 の動作について、第 1 1 図～第 1 5 図に示したフローチャートを参照しつつ説明する。第 1 1 図に示したステップ S F 1 では、CPU 6 1 0 は、通常命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。通常命令は、実施の形態 1 で説明した動作モード追加命令および論理回路データダウンロード命令以外の命令であって、CPU 6 1 0 で実行される命令である。

ステップ S F 2 では、CPU 6 1 0 は、動作モード追加命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。動作モード追加命令は、第 3 図に示した動作モード／命令対応表 4 0 0 の動作モードを追加するための命令である。

ステップ S F 3 では、CPU 6 1 0 は、論理回路データダウンロード命令が入力されたか否かを判断し、この場合、判断結果を「No」とし、ステップ S F 1 の判断を行う。論理回路データダウンロード命令は、インターネット 2 0 0 を介して、サーバ 5 0 0 から論理回路データをダウンロードするための命令である。以後、CPU 6 1 0 は、ステップ S F 1 ～ステップ S F 3 の判断を繰り返す。

そして、通常命令が入力されると、CPU 6 1 0 は、ステップ S F 1 の判断結果を「Yes」とする。ステップ S F 4 では、CPU 6 1 0 は、通常命令実行処理を実行する。

具体的には、第 1 2 図に示したステップ S G 1 では、命令入力部 3 1 1 (第 1 0 図参照) は、命令バスを介して入力された通常命令を命令使用可否判断部 3 1 4 および命令実行部 6 1 1 にフェッチする。ステップ S G 2 では、動作モード保持部 3 1 2 は、現時点で設定されている動作モードを使用可能命令保持部 3 1 3 へ通知する。ここで通知された動作モードは、第 3 図に示した「1」であるとする。

ステップ S G 3 では、使用可能命令保持部 3 1 3 は、通知された動作モードに

対応する命令群を使用可能命令群として命令使用可否判断部 3 1 4 へ通知する。
この場合の使用可能命令群は、第 3 図に示した動作モード = 1 に対応する命令 1
(0 x 1 1) ~ 命令 i (0 x e 7) である。

5 ステップ S G 4 では、命令使用可否判断部 3 1 4 は、ステップ S G 1 でフェッ
チされた通常命令が、当該動作モードで使用可能であるか否かを判断する。具体
的には、命令使用可否判断部 3 1 4 は、ステップ S G 3 で通知された使用可能命
令群に、ステップ S G 1 でフェッチされた通常命令が存在するか否かを判断し、
この場合、判断結果を「Y e s」とする。

10 ステップ S G 5 では、命令実行部 6 1 1 は、ステップ S G 1 でフェッチされた
通常命令 (使用可能命令) に対応する論理回路の生成を論理回路生成部 6 1 2 に
指示する。ステップ S G 6 では、論理回路生成部 6 1 2 は、当該通常命令に対応
する論理回路データに基づいて、命令実行部 6 1 1 に論理回路を生成する。

15 ステップ S G 7 では、命令実行部 6 1 1 は、データ入出力部 3 1 7 より、命令
実行に用いられるデータを取得する。ステップ S G 8 では、命令実行部 6 1 1 は、
生成された論理回路およびデータを用いて通常命令を実行する。ステップ S G 9
では、命令実行部 6 1 1 は、通常命令を実行した結果をデータ入出力部 3 1 7 を
経由して出力する。

20 一方、ステップ S G 4 の判断結果が「N o」である場合、すなわち、ステップ
S G 1 でフェッチされた通常命令が当該動作モード = 1 で使用不可である場合、
ステップ S G 1 0 では、命令使用可否判断部 3 1 4 は、権限違反または未定義命
令例外割り込み発生 (エラー) として処理する。

ここで、CPU 6 1 0 において、第 3 図に示した動作モード = 1 の命令群に含
まれない命令 n (0 x f 8) (動作モード = 0) を実行できるようにする場合に
は、動作モード = 1 を追加すればよい。以下では、動作モード追加処理について
25 説明する。

動作モード追加命令が入力されると、CPU 6 1 0 は、第 1 1 図に示したステ
ップ S F 2 の判断結果を「Y e s」とする。ステップ S F 5 では、CPU 6 1 0

は、動作モード追加処理を実行する。

具体的には、第 1 3 図に示したステップ S H 1 では、命令入力部 3 1 1（第 1 2 図参照）は、命令バスを介して入力された動作モード追加命令を命令使用可否判断部 3 1 4 および命令実行部 6 1 1 にフェッチする。ステップ S H 2 では、動作モード保持部 3 1 2 は、現時点で設定されている動作モード（この場合、動作モード = 1）を使用可能命令保持部 3 1 3 へ通知する。

ステップ S H 3 では、使用可能命令保持部 3 1 3 は、通知された動作モード = 1 に対応する命令 1（0 x 1 1）～命令 i（0 x e 7）を使用可能命令群として命令使用可否判断部 3 1 4 へ通知する。

10 ステップ S H 4 では、命令使用可否判断部 3 1 4 は、ステップ S C 4（第 6 図参照）と同様にして、ステップ S H 1 でフェッチされた動作モード追加命令が、当該動作モードで使用可能であるか否かを判断し、この場合、判断結果を「Y e s」とする。

15 ステップ S H 5 では、命令実行部 6 1 1 は、ステップ S H 1 でフェッチされた動作モード追加命令（使用可能命令）に対応する論理回路の生成を論理回路生成部 6 1 2 に指示する。ステップ S H 6 では、論理回路生成部 6 1 2 は、当該動作モード追加命令に対応する論理回路データに基づいて、命令実行部 6 1 1 に論理回路を生成する。

20 ステップ S H 7 では、命令実行部 6 1 1 は、データ入出力部 3 1 7 より、動作モードデータおよび命令群を取得する。この場合、動作モードデータは、追加すべき動作モードに対応する「0」（第 3 図参照）である。また、命令群は、第 3 図に示した動作モード = 0 に対応する命令 1（0 x 0 1）～命令 n（0 x f 8）である。

25 ステップ S H 8 では、命令実行部 6 1 1 は、動作モード保持部 3 1 2 に追加する動作モード = 0 を設定するとともに、使用可能命令保持部 3 1 3 に動作モード = 0 に対応する命令群を設定する。これにより、動作モード = 0 での命令群が使用可能となる。

一方、ステップSH4の判断結果が「No」である場合、ステップSH9では、命令使用可否判断部314は、権限違反または未定義命令例外割り込み発生（エラー）として処理する。

ここで、上述した動作モード追加処理により追加された動作モード=0に対応する命令群において、命令実行時に必要な論理回路データが論理回路データ保持部316に保持されていない場合、当該論理回路データをサーバ500からダウンロードする必要がある。以下では、論理回路データダウンロード処理について説明する。

この場合、第15図に示したステップSJ1では、第9図に示したダウンロード部620は、CPU610よりダウンロード要求があるか否かを判断し、この場合、判断結果を「No」として同判断を繰り返す。

そして、CPU610からダウンロード部620へ、当該論理回路データをダウンロードする要求があると、ダウンロード部620は、ステップSJ1の判断結果を「Yes」とする。ステップSJ2では、ダウンロード部620は、論理回路データ／論理回路データ番号対応表（図示略）に基づいて、CPU610から要求された論理回路データに対応する論理回路データ番号を指定する。

つぎに、ダウンロード部620は、当該論理回路データ番号に基づいて、インターネット200を介してサーバ500へ論理回路データダウンロード要求を出す。

これにより、ステップSJ3では、サーバ500のCPU510は、論理回路データ番号をキーとして、論理回路データ格納部520から当該論理回路データを読み出し、これをクライアント600のダウンロード部620へ転送する。

当該論理回路データが転送されると、ステップSJ4では、ダウンロード部620は、CPU610に対して、論理回路データダウンロード命令を発行した後、ステップSJ1の判断を行う。

そして、上記論理回路データダウンロード命令が入力されると、CPU610は、第11図に示したステップSF3の判断結果を「Yes」とする。ステップ

S F 6 では、C P U 6 1 0 は、論理回路データダウンロード処理を実行する。

具体的には、第 1 4 図に示したステップ S I 1 では、命令入力部 3 1 1（第 1 2 図参照）は、命令バスを介して入力された論理回路データダウンロード命令を命令使用可否判断部 3 1 4 および命令実行部 6 1 1 にフェッチする。ステップ S I 2 では、動作モード保持部 3 1 2 は、現時点で設定されている動作モード（この場合、動作モード = 0、1）を使用可能命令保持部 3 1 3 へ通知する。

ステップ S I 3 では、使用可能命令保持部 3 1 3 は、通知された動作モード = 0、1 に対応する命令 1（0 x 0 1）～命令 n（0 x f 8）、命令 1（0 x 1 1）～命令 i（0 x e 7）を使用可能命令群として命令使用可否判断部 3 1 4 へ通知する。

ステップ S I 4 では、命令使用可否判断部 3 1 4 は、ステップ S I 1 でフェッチされた論理回路データダウンロード命令が、当該動作モード 0、1 で使用可能であるか否かを判断し、この場合、判断結果を「Y e s」とする。

ステップ S I 5 では、命令実行部 6 1 1 は、ステップ S I 1 でフェッチされた論理回路データダウンロード命令（使用可能命令）に対応する論理回路の生成を論理回路生成部 6 1 2 に指示する。ステップ S I 6 では、論理回路生成部 6 1 2 は、当該論理回路データダウンロード命令に対応する論理回路データに基づいて、命令実行部 6 1 1 に論理回路を生成する。

ステップ S I 7 では、命令実行部 6 1 1 は、論理回路データダウンロード命令および生成された論理回路に基づいて、データ入出力部 3 1 7 およびデータバスを介してダウンロード部 6 2 0 から設定用の論理回路データを取得する。

ステップ S I 8 では、命令実行部 6 1 1 は、設定用の論理回路データを論理回路生成部 6 1 2 に設定する。これにより、前述した動作モード追加処理により追加された動作モード = 0 での命令群が使用可能となる。

一方、ステップ S I 4 の判断結果が「N o」である場合、すなわち、ステップ S I 1 でフェッチされた論理回路データダウンロード命令が当該動作モード = 0、1 で使用不可である場合、ステップ S I 9 では、命令使用可否判断部 3 1 4 は、

権限違反または未定義命令例外割り込み発生（エラー）として処理する。

以上説明したように、実施の形態２によれば、複数の動作モードのうち動的に指定された動作モードを第１０図に示した動作モード保持部３１２に追加し、追加された動作モードに対応する命令を使用可能命令保持部３１３に設定し、さらに、動作モード保持部３１２に保持された動作モードに対応し、命令の実行に用いられる論理回路を命令実行部６１１に生成するための論理回路データを外部のサーバ５００（第９図参照）から取得するようにしたので、セキュリティを維持しつつ拡張性を高めることができ、コストを低減させることができる。

（実施の形態３）

さて、前述した実施の形態１では、サーバ１００（第１図参照）からダウンロードされるファームウェアのセキュリティについて特に言及しなかったが、暗号化技術を用いてセキュリティを高める構成としてもよい。以下では、この構成例を実施の形態３として説明する。

第１６図は、本発明にかかる実施の形態３の構成を示すブロック図である。この図において、第１図の各部に対応する部分には同一の符号を付け、その説明を省略する。

第１６図に示したサーバ７００は、各種暗号化ファームウェアをクライアント８００へインターネット２００を介して提供する。サーバ７００において、ＣＰＵ７１０は、暗号化ファームウェア提供に関する制御を行う。

平文ファームウェア格納部７２０は、後述するＣＰＵ８１０での命令実行に用いられる平文ファームウェアを複数格納している。これらの平文ファームウェアは、平文ファームウェア番号に対応付けられて、平文ファームウェア格納部７２０に格納されている。ここで、実施の形態３での平文ファームウェアは、実施の形態１でのファームウェアと同一のものである。

暗号化部７３０は、ＣＰＵ７１０の制御の下で、ＲＳＡ（Rivest Shamir Adleman）暗号化方式や、ＤＥＳ（Data Encryption Standard）暗号化方式等により、平文ファームウェアを暗号化し、これを暗号化ファームウェアとして出力する。

クライアント８００は、インターネット２００に接続されており、インターネット２００を介して、サーバ７００から暗号化ファームウェアをダウンロードする機能と、暗号化ファームウェアを復号する機能と、復号された平文ファームウェアを用いて各種命令を実行し、結果を出力する機能とを備えている。

- ５ クライアント８００において、ＣＰＵ８１０は、暗号化ファームウェアを動的にダウンロードさせるための制御や、暗号化ファームウェアの復号、実施の形態１で説明した動作モードや命令群の設定等を行う。

ダウンロード部８２０は、ＣＰＵ８１０の制御により、サーバ７００から暗号化ファームウェアをダウンロードする。

- １０ 第１７図は、第１６図に示したＣＰＵ８１０の構成を示すブロック図である。この図において、第２図に対応する部分には同一の符号を付け、その説明を省略する。

第１７図に示したＣＰＵ８１０において、命令実行部８１１は、命令使用可否判断部３１４により使用可能と判断された命令を実行する。また、命令実行部８

- １５ １１は、当該命令の実行に用いられる平文ファームウェアをファームウェア保持部３１６より取得する。復号部８１２は、命令実行部８１１の制御の下で、ダウンロード部８２０（第１６図参照）によりダウンロードされた暗号化ファームウェアを復号し、復号結果を平文ファームウェアとしてファームウェア保持部３１６に保持させる。

- ２０ 実施の形態３において、ファームウェア保持部３１６は、動作モード保持部３１２に設定された動作モードでの命令群に対応する平文ファームウェアを保持する。

- この平文ファームウェアは、サーバ７００（第１６図参照）からダウンロードされた暗号化ファームウェアが復号されたものである。また、動作モードが追加された場合、ファームウェア保持部３１６には、新規の平文ファームウェアが保持される。

つぎに、実施の形態３の動作について、第１８図～第２０図に示したフローチ

ャートを参照しつつ説明する。第18図に示したステップSK1では、CPU810は、ステップSA1（第4図参照）と同様にして、通常命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。

5 ステップSK2では、CPU810は、ステップSA2（第4図参照）と同様にして、動作モード追加命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。

ステップSK3では、CPU810は、暗号化ファームウェアダウンロード命令が入力されたか否かを判断し、この場合、判断結果を「No」とし、ステップSK1の判断を行う。暗号化ファームウェアダウンロード命令は、インターネット200を介して、サーバ700から暗号化ファームウェアをダウンロードするための命令である。以後、CPU810は、ステップSK1～ステップSK3の判断を繰り返す。

そして、通常命令が入力されると、CPU810は、ステップSK1の判断結果を「Yes」とする。ステップSK4では、CPU810は、実施の形態1と同様にして、通常命令実行処理（第5図参照）を実行する。

また、動作モード追加命令が入力されると、CPU810は、ステップSK2の判断結果を「Yes」とする。ステップSK5では、CPU810は、実施の形態1と同様にして、動作モード追加処理（第6図参照）を実行する。

ここで、上述した動作モード追加処理により追加された動作モードに対応する命令群において、命令実行時に必要な平文ファームウェアがファームウェア保持部316に保持されていない場合、当該平文ファームウェアに対応する暗号化ファームウェアをサーバ700からダウンロードする必要がある。以下では、暗号化ファームウェアダウンロード処理について説明する。

この場合、第20図に示したステップSM1では、第16図に示したダウンロード部820は、CPU810よりダウンロード要求があるか否かを判断し、この場合、判断結果を「No」として同判断を繰り返す。

そして、CPU810からダウンロード部820へ、当該暗号化ファームウェア

アをダウンロードする要求があると、ダウンロード部 820 は、ステップ SM1 の判断結果を「Yes」とする。ステップ SM2 では、ダウンロード部 820 は、ファームウェア／ファームウェア番号対応表（図示略）に基づいて、CPU 810 から要求された暗号化ファームウェアに対応するファームウェア番号を指定する。つぎに、ダウンロード部 820 は、当該ファームウェア番号に基づいて、インターネット 200 を介してサーバ 700 へ暗号化ファームウェアダウンロード要求を出す。

これにより、ステップ SM3 では、サーバ 700 の CPU 710 は、ファームウェア番号をキーとして、平文ファームウェア格納部 720 から当該平文ファームウェアを読み出し、これを暗号化部 730 へ転送する。ステップ SM4 では、暗号化部 730 は、RSA 暗号化方式や DES 暗号化方式等により、上記平文ファームウェアを暗号化する。

ステップ SM5 では、CPU 710 は、インターネット 200 を介して、暗号化部 730 からの暗号化ファームウェアをクライアント 800 のダウンロード部 820 へ転送する。

当該暗号化ファームウェアが転送されると、ステップ SM6 では、ダウンロード部 820 は、CPU 810 に対して、暗号化ファームウェアダウンロード命令を発行した後、ステップ SM1 の判断を行う。

そして、上記暗号化ファームウェアダウンロード命令が入力されると、CPU 810 は、第 18 図に示したステップ SK3 の判断結果を「Yes」とする。ステップ SK6 では、CPU 810 は、暗号化ファームウェアダウンロード処理を実行する。

具体的には、第 19 図に示したステップ SL1 では、命令入力部 311（第 17 図参照）は、命令バスを介して入力された暗号化ファームウェアダウンロード命令を命令使用可否判断部 314 および命令実行部 811 にフェッチする。ステップ SL2 では、動作モード保持部 312 は、現時点で設定されている動作モードを使用可能命令保持部 313 へ通知する。

ステップS L 3では、使用可能命令保持部3 1 3は、通知された動作モードに対応する命令群を使用可能命令群として命令使用可否判断部3 1 4へ通知する。

5 ステップS L 4では、命令使用可否判断部3 1 4は、ステップS L 1でフェッチされた暗号化ファームウェアダウンロード命令が、当該動作モードで使用可能であるか否かを判断し、この場合、判断結果を「Y e s」とする。

ステップS L 5では、命令実行部8 1 1は、ステップS L 1でフェッチされた暗号化ファームウェアダウンロード命令（使用可能命令）に対応する実行用の平文ファームウェアをファームウェア保持部3 1 6から取得する。

10 ステップS L 6では、命令実行部8 1 1は、暗号化ファームウェアダウンロード命令およびこれに対応する実行用の平文ファームウェアに基づいて、データ入出力部3 1 7およびデータベースを介してダウンロード部8 2 0から設定用の暗号化ファームウェアを取得する。

15 ステップS L 7では、命令実行部8 1 1は、復号部8 1 2へ暗号化ファームウェアの復号を指示する。ステップS L 8では、復号部8 1 2は、暗号化ファームウェアを復号する。ステップS L 9では、復号部8 1 2は、命令実行部8 1 1の制御の下で、復号された平文ファームウェアをファームウェア保持部3 1 6に設定する。これにより、動作モード追加処理により追加された動作モードでの命令群が使用可能となる。

20 一方、ステップS L 4の判断結果が「N o」である場合、ステップS L 10では、命令使用可否判断部3 1 4は、権限違反または未定義命令例外割り込み発生（エラー）として処理する。

以上説明したように、実施の形態3によれば、暗号化ファームウェアを外部のサーバ7 0 0（第1 6図参照）から取得した後、該暗号化ファームウェアを復号部8 1 2（第1 7図参照）で復号するようにしたので、ファームウェア取得中の
25 セキュリティを高めることができる。

（実施の形態4）

さて、前述した実施の形態3では、ファームウェアを暗号化してセキュリティ

を高める構成例について説明したが、電子署名技術を用いてセキュリティを高める構成としてもよい。以下では、この構成例を実施の形態4として説明する。

第21図は、本発明にかかる実施の形態4の構成を示すブロック図である。この図において、第1図の各部に対応する部分には同一の符号を付け、その説明を省略する。

第21図に示したサーバ900は、各種電子署名付きファームウェアをクライアント1000へインターネット200を介して提供する。サーバ900において、CPU910は、電子署名付きファームウェア提供に関する制御を行う。

電子署名部920は、CPU910の制御の下で、電子署名付きのファームウェアを生成する。電子署名は、ファームウェアが正当な発信者から発信され、途中で改竄などが行なわれていないことを示すためのセキュリティ技術である。

クライアント1000は、インターネット200に接続されており、インターネット200を介して、サーバ900から電子署名付きファームウェアをダウンロードする機能と、電子署名付きファームウェアを認証する機能と、認証されたファームウェアを用いて各種命令を実行し、結果を出力する機能とを備えている。

クライアント1000において、CPU1010は、電子署名付きファームウェアを動的にダウンロードさせるための制御や、電子署名付きファームウェアの認証、実施の形態1で説明した動作モードや命令群の設定等を行う。

ダウンロード部1020は、CPU1010の制御により、サーバ900から電子署名付きファームウェアをダウンロードする。

第22図は、第21図に示したCPU1010の構成を示すブロック図である。この図において、第2図に対応する部分には同一の符号を付け、その説明を省略する。

第22図に示したCPU1010において、命令実行部1011は、命令使用可否判断部314により使用可能と判断された命令を実行する。また、命令実行部1011は、当該命令の実行に用いられるファームウェアをファームウェア保持部316より取得する。認証部1012は、命令実行部1011の制御の下で、

ダウンロード部 1020（第 21 図参照）によりダウンロードされた電子署名付きファームウェアの認証を行い、認証結果が OK である場合、ファームウェアをファームウェア保持部 316 に保持させる。

つぎに、実施の形態 4 の動作について、第 23 図～第 25 図に示したフローチャートを参照しつつ説明する。

第 23 図に示したステップ SN1 では、CPU 1010 は、ステップ SA1（第 4 図参照）と同様にして、通常命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。

ステップ SN2 では、CPU 1010 は、ステップ SA2（第 4 図参照）と同様にして、動作モード追加命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。

ステップ SN3 では、CPU 1010 は、電子署名付きファームウェアダウンロード命令が入力されたか否かを判断し、この場合、判断結果を「No」とし、ステップ SN1 の判断を行う。電子署名付きファームウェアダウンロード命令は、インターネット 200 を介して、サーバ 900 から電子署名付きファームウェアをダウンロードするための命令である。以後、CPU 1010 は、ステップ SN1～ステップ SN3 の判断を繰り返す。

そして、通常命令が入力されると、CPU 1010 は、ステップ SN1 の判断結果を「Yes」とする。ステップ SN4 では、CPU 1010 は、実施の形態 1 と同様にして、通常命令実行処理（第 5 図参照）を実行する。

また、動作モード追加命令が入力されると、CPU 1010 は、ステップ SN2 の判断結果を「Yes」とする。ステップ SN5 では、CPU 1010 は、実施の形態 1 と同様にして、動作モード追加処理（第 6 図参照）を実行する。

ここで、上述した動作モード追加処理により追加された動作モードに対応する命令群において、命令実行時に必要なファームウェアがファームウェア保持部 316 に保持されていない場合、当該ファームウェアに対応する電子署名付きファームウェアをサーバ 900 からダウンロードする必要がある。以下では、電子署

名付きファームウェアダウンロード処理について説明する。

この場合、第25図に示したステップSP1では、第21図に示したダウンロード部1020は、CPU1010よりダウンロード要求があるか否かを判断し、この場合、判断結果を「No」として同判断を繰り返す。

- 5 そして、CPU1010からダウンロード部1020へ、当該電子署名付きファームウェアをダウンロードする要求があると、ダウンロード部1020は、ステップSP1の判断結果を「Yes」とする。ステップSP2では、ダウンロード部1020は、ファームウェア／ファームウェア番号対応表（図示略）に基づいて、CPU1010から要求されたファームウェアに対応するファームウェア
- 10 番号を指定する。つぎに、ダウンロード部1020は、当該ファームウェア番号に基づいて、インターネット200を介してサーバ900へ電子署名付きファームウェアダウンロード要求を出す。

- これにより、ステップSP3では、サーバ900のCPU910は、ファームウェア番号をキーとして、ファームウェア格納部130から当該ファームウェア
- 15 を読み出し、これを電子署名部920へ転送する。ステップSP4では、電子署名部920は、電子署名付きファームウェアを生成する。

ステップSP5では、CPU910は、インターネット200を介して、電子署名部920からの電子署名付きファームウェアをクライアント1000のダウンロード部1020へ転送する。

- 20 当該電子署名付きファームウェアが転送されると、ステップSP6では、ダウンロード部1020は、CPU1010に対して、電子署名付きファームウェアダウンロード命令を発行した後、ステップSP1の判断を行う。

- そして、上記電子署名付きファームウェアダウンロード命令が入力されると、CPU1010は、第23図に示したステップSN3の判断結果を「Yes」と
- 25 する。ステップSN6では、CPU1010は、電子署名付きファームウェアダウンロード処理を実行する。

具体的には、第24図に示したステップSO1では、命令入力部311（第2

2 図参照) は、命令バスを介して入力された電子署名付きファームウェアダウンロード命令を命令使用可否判断部 3 1 4 および命令実行部 1 0 1 1 にフェッチする。ステップ S O 2 では、動作モード保持部 3 1 2 は、現時点で設定されている動作モードを使用可能命令保持部 3 1 3 へ通知する。

- 5 ステップ S O 3 では、使用可能命令保持部 3 1 3 は、通知された動作モードに対応する命令群を使用可能命令群として命令使用可否判断部 3 1 4 へ通知する。

ステップ S O 4 では、命令使用可否判断部 3 1 4 は、ステップ S O 1 でフェッチされた電子署名付きファームウェアダウンロード命令が、当該動作モードで使用可能であるか否かを判断し、この場合、判断結果を「Y e s」とする。

- 10 ステップ S O 5 では、命令実行部 1 0 1 1 は、ステップ S O 1 でフェッチされた電子署名付きファームウェアダウンロード命令（使用可能命令）に対応する実行用のファームウェアをファームウェア保持部 3 1 6 から取得する。

- ステップ S O 6 では、命令実行部 1 0 1 1 は、電子署名付きファームウェアダウンロード命令およびこれに対応する実行用のファームウェアに基づいて、データ入出力部 3 1 7 およびデータベースを介してダウンロード部 1 0 2 0 から設定用の電子署名付きファームウェアを取得する。
- 15

ステップ S O 7 では、命令実行部 1 0 1 1 は、認証部 1 0 1 2 へ電子署名付きファームウェアの認証を指示する。ステップ S O 8 では、認証部 1 0 1 2 は、電子署名付きファームウェアを認証し、認証結果を命令実行部 1 0 1 1 へ通知する。

- 20 ステップ S O 9 では、命令実行部 1 0 1 1 は、認証部 1 0 1 2 での認証結果が O K であるか否かを判断する。

認証結果が N G である場合、すなわち、設定用のファームウェアが改竄等されている場合、命令実行部 1 0 1 1 は、ステップ S O 9 の判断結果を「N o」として、設定を中止し、第 2 3 図に示したメインルーチンへ戻る。

- 25 一方、認証結果が O K である場合、命令実行部 1 0 1 1 は、ステップ S O 9 の判断結果を「Y e s」とする。ステップ S O 1 0 では、認証部 1 0 1 2 は、命令実行部 1 0 1 1 の制御の下で、認証されたファームウェアをファームウェア保持

部 3 1 6 に設定する。これにより、動作モード追加処理により追加された動作モードでの命令群が使用可能となる。

一方、ステップ S O 4 の判断結果が「N o」である場合、ステップ S O 1 1 では、命令使用可否判断部 3 1 4 は、権限違反または未定義命令例外割り込み発生
5 (エラー) として処理する。

以上説明したように、実施の形態 4 によれば、電子署名付きファームウェアを外部のサーバ 9 0 0 (第 2 1 図参照) から取得した後、該署名付きファームウェアを認証部 1 0 1 2 (第 2 2 図参照) で認証するようにしたので、ファームウェア取得中の改竄等を防止することができる。

10 (実施の形態 5)

さて、前述した実施の形態 1 では、命令実行時に、CPU 内部に保持されている資源 (例えば、暗号鍵、署名鍵、証明書等) へのアクセス制御について特に言及しなかったが、上記アクセス制御を行う構成としてもよい。以下では、この構成例を実施の形態 5 として説明する。

15 第 2 6 図は、本発明にかかる実施の形態 5 の構成を示すブロック図である。この図において、第 1 図の各部に対応する部分には同一の符号を付け、その説明を省略する。

第 2 6 図に示したクライアント 1 1 0 0 は、インターネット 2 0 0 に接続されており、インターネット 2 0 0 を介して、サーバ 1 0 0 からファームウェアをダウンロードする機能と、ファームウェアを用いて各種命令を実行し、結果を出力する機能とを備えている。
20

クライアント 1 1 0 0 において、CPU 1 1 1 0 は、ファームウェアを動的にダウンロードさせるための制御や、後述する動作モードや命令群の設定、上述したアクセス制御等を行う。

25 第 2 7 図は、第 2 6 図に示した CPU 1 1 1 0 の構成を示すブロック図である。この図において、第 2 図の各部に対応する部分には同一の符号を付け、その説明を省略する。命令実行部 1 1 1 1 は、命令使用可否判断部 3 1 4 により使用可能

と判断された命令を実行する。また、命令実行部 1 1 1 1 は、当該命令の実行に用いられるファームウェアをファームウェア保持部 3 1 6 より取得する。さらに、命令実行部 1 1 1 1 は、命令の種類によっては、CPU 1 1 1 0 内の資源（暗号鍵、署名鍵等）にアクセスする。例えば、実行命令が暗号化命令の場合には、命令実行部 1 1 1 1 は、暗号鍵にアクセスし、この暗号鍵を使ってデータを暗号化する。

暗号鍵保持部 1 1 1 3₁、署名鍵保持部 1 1 1 3₂、証明書保持部 1 1 1 3₃、CPU・ID 保持部 1 1 1 3₄、…には、資源としての暗号鍵、署名鍵、証明書、CPU・ID、…がそれぞれ保持されている。例えば、暗号鍵は、データを暗号化する際に用いられる。署名鍵は、データに電子署名を施す際に用いられる。

アクセス制御部 1 1 1 2 は、命令実行部 1 1 1 1 が資源にアクセスする場合に、第 2 8 図に示した動作モード／資源対応表 1 2 0 0 の動作モードに応じて、アクセスの許可／拒絶を判断する。

動作モード／資源対応表 1 2 0 0 において、動作モードは、「0」～「k」とされており、動作モード／命令対応表 4 0 0（第 3 図参照）の動作モードに対応している。

アクセス可能数は、動作モード毎に設定されており、当該動作モード時に命令実行部 1 1 1 1 でアクセス可能な資源の数である。

例えば、動作モード＝0 の場合には、アクセス可能数が n である。すなわち、動作モード 0 の場合には、資源 1（暗号鍵）～資源 n（CPU・ID）という都合 n 種類の資源に命令実行部 1 1 1 1 がアクセス可能となる。

また、動作モード＝1 の場合には、アクセス可能数が i である。すなわち、動作モード 1 の場合には、資源 1（暗号鍵）～資源 i（CPU・ID）という都合 i 種類の資源に命令実行部 1 1 1 1 がアクセス可能である。

同様にして、動作モード＝k の場合には、アクセス可能数が 1 である。すなわち、動作モード k の場合には、資源 1（署名鍵）という都合 1 種類の資源に命令

実行部 1 1 1 1 がアクセス可能である。また、動作モード = k のみが設定されている場合、命令実行部 1 1 1 1 は、資源 1（署名鍵）以外の資源にアクセスできない。

つぎに、実施の形態 5 の動作について、第 4 図、第 29 図～第 31 図に示した
5 フローチャートを参照しつつ説明する。第 4 図に示したステップ SA1 では、CPU 1 1 1 0 は、通常命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。ステップ SA2 では、CPU 1 1 1 0 は、動作モード追加命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。

ステップ SA3 では、CPU 1 1 1 0 は、ファームウェアダウンロード命令が
10 入力されたか否かを判断し、この場合、判断結果を「No」とする。以後、CPU 1 1 1 0 は、ステップ SA1～ステップ SA3 の判断を繰り返す。

そして、通常命令が入力されると、CPU 1 1 1 0 は、ステップ SA1 の判断結果を「Yes」とする。ステップ SA4 では、CPU 1 1 1 0 は、通常命令実行処理を実行する。

15 具体的には、第 29 図に示したステップ SQ1 では、命令入力部 3 1 1（第 27 図参照）は、命令バスを介して入力された通常命令を命令使用可否判断部 3 1 4 および命令実行部 1 1 1 1 にフェッチする。ステップ SQ2 では、動作モード保持部 3 1 2 は、現時点で設定されている動作モードを使用可能命令保持部 3 1 3 およびアクセス制御部 1 1 1 2 へ通知する。ここで通知された動作モードは、
20 第 3 図および第 28 図に示した「1」であるとする。

ステップ SQ3 では、使用可能命令保持部 3 1 3 は、通知された動作モードに対応する命令群を使用可能命令群として命令使用可否判断部 3 1 4 へ通知する。この場合の使用可能命令群は、第 3 図に示した動作モード = 1 に対応する命令 1（0 x 1 1）～命令 i（0 x e 7）である。

25 ステップ SQ4 では、命令使用可否判断部 3 1 4 は、ステップ SQ1 でフェッチされた通常命令が、当該動作モードで使用可能であるか否かを判断する。具体的には、命令使用可否判断部 3 1 4 は、ステップ SQ3 で通知された使用可能命

令群に、ステップSQ1でフェッチされた通常命令が存在するか否かを判断し、この場合、判断結果を「Yes」とする。

ステップSQ5では、命令実行部1111から資源（暗号鍵、署名鍵、証明書、CPU・ID等）へのアクセスを制御するためのアクセス制御処理が実行される。

- 5 具体的には、第30図に示したステップSR1では、命令実行部1111は、通常命令の実行に際して資源へのアクセスが必要であるか否かを判断する。

この場合、通常命令が暗号化であるとし、資源として暗号鍵が必要である。従って、命令実行部1111は、ステップSR1の判断結果を「Yes」とする。なお、ステップSR1の判断結果が「No」である場合、命令実行部1111は、

- 10 第29図に示したステップSQ6の処理を実行する。

ステップSR2では、命令実行部1111は、アクセス制御部1112へ資源（暗号鍵）を通知する。ステップSR3では、アクセス制御部1112は、動作モード／資源対応表1200（第28図参照）を参照して、現在の動作モード＝1で、ステップSR2で通知された資源（暗号鍵）に対して命令実行部1111

15 がアクセス可能であるか否かを判断する。

- 具体的には、アクセス制御部1112は、第28図に示した動作モード＝1に対応する資源1（暗号鍵）～資源i（CPU・ID）に、ステップSR2で通知された資源（暗号鍵）が含まれているか否かを判断し、この場合、判断結果を「Yes」とする。ステップSR4では、アクセス制御部1112は、命令実行部1111に対して資源（暗号鍵）へのアクセスを許可する。
- 20

一方、ステップSR3の判断結果が「No」である場合、ステップSR5では、アクセス制御部1112は、命令実行部1111に対して資源（暗号鍵）へのアクセスを拒絶し、権限違反例外割り込み発生（エラー）として処理する。

- 第29図に戻り、ステップSQ6では、命令実行部1111は、ステップSQ1でフェッチされた通常命令（使用可能命令）に対応するファームウェアをファームウェア保持部316から取得する。
- 25

ステップSQ7では、命令実行部1111は、データ入出力部317より、命

令実行に用いられるデータを取得する。この場合には、命令実行部 1 1 1 1 は、アクセス制御部 1 1 1 2 により許可された資源としての暗号鍵（暗号鍵保持部 1 1 1 3、）にアクセスし、暗号鍵も取得する。

5 ステップ S Q 8 では、命令実行部 1 1 1 1 は、ファームウェア、データ、資源（暗号鍵）を用いて通常命令を実行する。ステップ S Q 9 では、命令実行部 1 1 1 1 は、通常命令を実行した結果をデータ入出力部 3 1 7 を経由して出力する。

一方、ステップ S Q 4 の判断結果が「N o」である場合、すなわち、ステップ S Q 1 でフェッチされた通常命令が当該動作モード＝1 で使用不可である場合、ステップ S Q 1 0 では、命令使用可否判断部 3 1 4 は、権限違反または未定義命令例外割り込み発生（エラー）として処理する。

つぎに、動作モード追加処理について説明する。動作モード追加命令が入力されると、CPU 1 1 1 0 は、第 4 図に示したステップ S A 2 の判断結果を「Y e s」とする。ステップ S A 5 では、CPU 1 1 1 0 は、動作モード追加処理を実行する。

15 具体的には、第 3 1 図に示したステップ S S 1 では、命令入力部 3 1 1（第 2 7 図参照）は、命令バスを介して入力された動作モード追加命令を命令使用可否判断部 3 1 4 および命令実行部 1 1 1 1 にフェッチする。ステップ S S 2 では、動作モード保持部 3 1 2 は、現時点で設定されている動作モード（この場合、動作モード＝1）を使用可能命令保持部 3 1 3 へ通知する。

20 ステップ S S 3 では、使用可能命令保持部 3 1 3 は、通知された動作モード＝1 に対応する命令 1（0 x 1 1）～命令 i（0 x e 7）を使用可能命令群として命令使用可否判断部 3 1 4 へ通知する。

ステップ S S 4 では、命令使用可否判断部 3 1 4 は、ステップ S S 1 でフェッチされた動作モード追加命令が、当該動作モードで使用可能であるか否かを判断し、この場合、判断結果を「Y e s」とする。

25 なお、ステップ S S 4 の判断結果が「N o」である場合、すなわち、ステップ S S 1 でフェッチされた動作モード追加命令が当該動作モード＝1 で使用不可で

ある場合、ステップS S 1 0では、命令使用可否判断部3 1 4は、権限違反または未定義命令例外割り込み発生（エラー）として処理する。

5 ステップS S 5では、命令実行部1 1 1 1は、ステップS S 1でフェッチされた動作モード追加命令（使用可能命令）に対応するファームウェアをファームウェア保持部3 1 6から取得する。

ステップS S 6では、命令実行部1 1 1 1は、データ入出力部3 1 7より、追加動作モードデータおよび命令群を取得する。この場合、追加動作モードデータは、追加すべき動作モードに対応する「0」（第3図参照）とする。また、命令群は、第3図に示した動作モード=0に対応する命令1（0 x 0 1）～命令n
10 （0 x f 8）である。

ステップS S 7では、命令実行部1 1 1 1は、動作モード保持部3 1 2に現在設定されている動作モード（=1）を確認する。ステップS S 8では、命令実行部1 1 1 1は、追加動作モード（=0）が現在の動作モード（=1）より低モードであるか否かを判断する。言い換えれば、命令実行部1 1 1 1は、追加動作モードにより、使用可能命令数が増加するか否かを判断する。
15

すなわち、命令実行部1 1 1 1は、動的に指定された追加の動作モードの命令数が、動作モード保持部3 1 2（第27図参照）に既に保持されている動作モードの命令数より多いか否かを判断する。

この場合、命令実行部1 1 1 1は、ステップS S 8の判断結果を「Y e s」と
20 する。ステップS S 9では、命令実行部1 1 1 1は、動作モード保持部3 1 2に追加する動作モード=0を設定するとともに、使用可能命令保持部3 1 3に動作モード=0に対応する命令群を設定する。これにより、動作モード=0での命令群が使用可能となる。

一方、ステップS S 8の判断結果が「N o」である場合、ステップS S 1 1では、命令実行部1 1 1 1は、動作モードの追加を中止し、権限違反例外割り込み発生（エラー）として処理する。
25

また、ファームウェアダウンロード命令が入力された場合、C P U 1 1 1 0は、

第4図に示したステップSA3の判断結果を「Yes」とする。ステップSA6では、CPU1110は、実施の形態1と同様にして、ファームウェアダウンロード処理（第7図参照）を実行する。

以上説明したように、実施の形態5によれば、動作モードに応じて、命令の実行に際して利用される各種資源（暗号鍵、署名鍵、証明書、CPU・ID等）に対するアクセス制御をアクセス制御部1112（第27図参照）で行うようにしたので、動作モードに応じて動的に資源を割り当てることができる。

また、実施の形態5によれば、動的に指定された追加の動作モードの命令数が、動作モード保持部312（第27図参照）に既に保持されている動作モードの命令数より多い場合に限り、動的に指定された動作モードを動作モード保持部312に追加するようにしたので、より厳しい条件での動作モードの追加が可能となり、セキュリティをさらに高めることができる。

（実施の形態6）

さて、前述した実施の形態1では、CPU310（第1図参照）外部のオペレーティングシステムにより動作モード追加およびファームウェアダウンロードの指示を行うように構成してもよい。以下では、この構成例を実施の形態6として説明する。

第32図は、本発明にかかる実施の形態6の構成を示すブロック図である。この図において、第1図の各部に対応する部分には同一の符号を付ける。第32図に示したクライアント1300は、インターネット200に接続されており、インターネット200を介して、サーバ100からファームウェアをダウンロードする機能と、ファームウェアを用いて各種命令を実行し、結果を出力する機能を備えている。

クライアント1300において、オペレーティングシステム1310は、動作モード追加およびファームウェアダウンロードを指示するためのシステムである。動作モードファイル格納部1320には、第33図に示した動作モードファイル1321。～1321_kが格納されている。これらの動作モードファイル132

1。～1321_kは、第3図に示した動作モード／命令対応表400に対応するファイルである。

動作モードファイル1321₀は、動作モードデータ1322₀、使用可能命令数データ1323₀、および命令／ファームウェア番号データ1324₀から
5 構成されている。動作モードデータ1322₀は、第3図に示した動作モード＝0を表すデータである。

使用可能命令数データ1323₀は、第3図に示した使用可能命令数＝nを表すデータである。命令／ファームウェア番号データ1324₀は、第3図に示した命令1(0x01)～命令n(0x8f)、およびこれらに対応するファーム
10 ウェアを指定するためのファームウェア番号のデータである。

動作モードファイル1321₁～1321_kは、上述した動作モードファイル1321₀と同一のデータ構造とされており、動作モード1～kに関するデータから構成されている。

なお、実施の形態6において、第32図に示したダウンロード部330は、ファームウェアダウンロード命令を発行せず、ダウンロード機能のみを備えている。
15 ファームウェアダウンロード命令は、オペレーティングシステム1310により発行される。

第34図は、第32図に示したオペレーティングシステム1310およびCPU310の構成を示すブロック図である。この図において、第2図および第32
20 図に対応する部分には同一の符号を付け、その説明を省略する。

第34図に示したオペレーティングシステム1310において、プロセス管理部1311は、シェルプロセス1312(動作モード追加、ファームウェアダウンロード等)や子プロセス1313を管理する。

ファイルシステム1314は、プロセス管理部1311の制御の下で動作モードファイル格納部1320から動作モードファイルを読み出す。動作モード追加
25 指示部1315は、プロセス管理部1311の制御の下で、CPU310における動作モード追加を指示する。

ファームウェアダウンロード指示部 1 3 1 6 は、プロセス管理部 1 3 1 1 の制御の下でサーバ 1 0 0（第 3 2 参照）からのファームウェアのダウンロードを指示する。

つぎに、実施の形態 6 の動作について、第 4 図～第 8 図および第 3 5 図に示したフローチャートを参照しつつ説明する。第 4 図に示したステップ S A 1 では、CPU 3 1 0 は、通常命令が入力されたか否かを判断し、この場合、判断結果を「N o」とする。

ステップ S A 2 では、CPU 3 1 0 は、動作モード追加命令が入力されたか否かを判断し、この場合、判断結果を「N o」とする。ステップ S A 3 では、CPU 3 1 0 は、ファームウェアダウンロード命令が入力されたか否かを判断し、この場合、判断結果を「N o」とし、ステップ S A 1 ～ステップ S A 3 の判断を繰り返す。

そして、通常命令が入力されると、CPU 3 1 0 は、ステップ S A 1 の判断結果を「Y e s」とする。ステップ S A 4 では、CPU 3 1 0 は、実施の形態 1 と同様にして通常命令実行処理（第 5 図参照）を実行する。

ここで、動作モード（例えば、動作モード＝0）を追加する場合、第 3 5 図に示したステップ S T 1 では、第 3 4 図に示したオペレーティングシステム 1 3 1 0 のシェルプロセス 1 3 1 2 は、プロセス管理部 1 3 1 1 にプロセス起動を指示する。

ステップ S T 2 では、プロセス管理部 1 3 1 1 は、ファイルシステム 1 3 1 4 に対して、第 3 3 図に示した動作モードファイル格納部 1 3 2 0 から、追加すべき動作モード＝0に対応する動作モードファイル 1 3 2 1。を読み出すことを指示する。

ステップ S T 3 では、ファイルシステム 1 3 1 4 は、動作モードファイル格納部 1 3 2 0 から動作モードファイル 1 3 2 1。を読み出す。ステップ S T 4 では、プロセス管理部 1 3 1 1 は、動作モード追加指示部 1 3 1 5 へ動作モード＝0の追加を指示する。ステップ S T 5 では、動作モード追加指示部 1 3 1 5 は、動作

モード指示処理として、CPU 310に対して、動作モード追加命令を発行する。

そして、動作モード追加命令が入力されると、CPU 310は、第4図に示したステップSA2の判断結果を「Yes」とする。ステップSA5では、CPU 310は、動作モード追加処理を実行する。

- 5 具体的には、第6図に示したステップSC1では、命令入力部311（第34図参照）は、命令バスを介して入力された動作モード追加命令を命令使用可否判断部314および命令実行部315にフェッチする。

ステップSC2では、動作モード保持部312は、現時点で設定されている動作モード（この場合、動作モード＝1）を使用可能命令保持部313へ通知する。

- 10 ステップSC3では、使用可能命令保持部313は、通知された動作モード＝1に対応する使用可能命令群を命令使用可否判断部314へ通知する。

ステップSC4では、命令使用可否判断部314は、ステップSC1でフェッチされた動作モード追加命令が、当該動作モードで使用可能であるか否かを判断し、この場合、判断結果を「Yes」とする。

- 15 ステップSC5では、命令実行部315は、ステップSC1でフェッチされた動作モード追加命令（使用可能命令）に対応するファームウェアをファームウェア保持部316から取得する。

- ステップSC6では、命令実行部315は、データ入出力部317より、動作モードデータおよび命令群を取得する。この場合、動作モードデータは、追加すべき動作モードに対応する「0」（第3図参照）である。また、命令群は、第3図に示した動作モード＝0に対応する命令1（0x01）～命令n（0xf8）である。
- 20

- ステップSC7では、命令実行部315は、動作モード保持部312に追加する動作モード＝0を設定するとともに、使用可能命令保持部313に動作モード＝0に対応する命令群を設定する。これにより、動作モード＝0での命令群が使用可能となる。
- 25

第35図に戻り、ステップST6では、プロセス管理部1311は、ファイル

システム 1 3 1 4 に対して、第 3 3 図に示した動作モードファイル格納部 1 3 2 0 から、追加された動作モード=0 に対応する動作モードファイル 1 3 2 1。を読み出すことを指示する。

5 ステップ S T 7 では、ファイルシステム 1 3 1 4 は、動作モードファイル格納部 1 3 2 0 から第 3 3 図に示した動作モードファイル 1 3 2 1。を読み出す。ステップ S T 8 では、プロセス管理部 1 3 1 1 は、第 3 3 図に示した動作モードファイル 1 3 2 1。の命令／ファームウェア番号データ 1 3 2 4。をファームウェアダウンロード指示部 1 3 1 6 へ渡し、ダウンロードを指示させる。

10 これにより、ファームウェアダウンロード指示部 1 3 1 6 は、CPU 3 1 0 に対して、ファームウェアダウンロード命令を発行するとともに、命令／ファームウェア番号データ 1 3 2 4。をデータ入出力部 3 1 7 へ出力する。

そして、上記ファームウェアダウンロード命令が入力されると、CPU 3 1 0 は、第 4 図に示したステップ S A 3 の判断結果を「Y e s」とする。ステップ S A 6 では、CPU 3 1 0 は、ファームウェアダウンロード処理を実行する。

15 具体的には、第 7 図に示したステップ S D 1 では、命令入力部 3 1 1（第 3 4 図参照）は、命令バスを介して入力されたファームウェアダウンロード命令を命令使用可否判断部 3 1 4 および命令実行部 3 1 5 にフェッチする。ステップ S D 2 では、動作モード保持部 3 1 2 は、現時点で設定されている動作モードを使用可能命令保持部 3 1 3 へ通知する。

20 ステップ S D 3 では、使用可能命令保持部 3 1 3 は、通知された動作モードに対応する使用可能命令群を命令使用可否判断部 3 1 4 へ通知する。

ステップ S D 4 では、命令使用可否判断部 3 1 4 は、ステップ S D 1 でフェッチされたファームウェアダウンロード命令が、当該動作モードで使用可能であるか否かを判断する。具体的には、命令使用可否判断部 3 1 4 は、ステップ S D 3
25 で通知された使用可能命令群に、ステップ S D 1 でフェッチされたファームウェアダウンロード命令が存在するか否かを判断し、この場合、判断結果を「Y e s」とする。

ステップSD 5では、命令実行部315は、ステップSD 1でフェッチされたファームウェアダウンロード命令（使用可能命令）に対応する実行用のファームウェアをファームウェア保持部316から取得する。

5 ステップSD 6では、命令実行部315は、ファームウェアダウンロード命令およびこれに対応する実行用のファームウェアに基づいて、データ入出力部317およびデータバスを介してダウンロード部330から設定用のファームウェアを取得する。

具体的には、命令実行部315は、第32図に示したダウンロード部330へ命令／ファームウェア番号データ1324。（第33図参照）を出力するとともに、
10 に、ダウンロード要求を出す。これにより、ダウンロード部330は、第8図に示したステップSE 1の判断結果を「Yes」とする。

ステップSE 2では、ダウンロード部330は、命令／ファームウェア番号データ1324。に基づいて、要求されたファームウェアに対応するファームウェア番号を指定する。つぎに、ダウンロード部330は、当該ファームウェア番号
15 に基づいて、インターネット200を介してサーバ100へファームウェアダウンロード要求を出す。

これにより、ステップSE 3では、サーバ100のCPU110は、ファームウェア番号をキーとして、ファームウェア格納部130から当該ファームウェアを読み出し、これをクライアント1300のダウンロード部330へ転送する。
20 なお、実施の形態6では、ステップSE 4がスキップされる。

そして、第34図に示した命令実行部315は、ダウンロード部330から設定用のファームウェアを取得する。

第7図に戻り、ステップSD 7では、命令実行部315は、設定用のファームウェアをファームウェア保持部316に設定する。これにより、前述した動作モード追加処理により追加された動作モードでの命令群が使用可能となる。
25

以上説明したように、実施の形態6によれば、実施の形態1と同様の効果を奏する。

(実施の形態 7)

さて、前述した実施の形態 6 では、CPU 310 (第 32 図参照) 外部のオペレーティングシステムにより動作モード追加の指示、ファームウェアダウンロードの指示を行う構成例について説明したが、動作モードの削除の指示およびファームウェアアンロード指示も行うように構成してもよい。以下では、この構成例を実施の形態 7 として説明する。

第 36 図は、本発明にかかる実施の形態 7 の構成を示すブロック図である。この図において、第 32 図の各部に対応する部分には同一の符号を付ける。第 36 図に示したクライアント 1400 は、インターネット 200 に接続されており、インターネット 200 を介して、サーバ 100 からファームウェアをダウンロードする機能と、ファームウェアをアンロードする機能と、ファームウェアを用いて各種命令を実行し、結果を出力する機能とを備えている。

クライアント 1400 において、オペレーティングシステム 1420 は、動作モード追加、動作モード削除、ファームウェアダウンロードおよびファームウェアアンロードを指示するためのシステムである。

なお、実施の形態 7 において、第 36 図に示したダウンロード部 330 は、ファームウェアダウンロード命令を発行せず、ダウンロード機能のみを備えている。ファームウェアダウンロード命令は、オペレーティングシステム 1420 により発行される。

第 37 図は、第 36 図に示したオペレーティングシステム 1420 および CPU 1410 の構成を示すブロック図である。この図において、第 34 図に対応する部分には同一の符号を付け、その説明を省略する。

第 37 図に示したオペレーティングシステム 1420 において、プロセス管理部 1421 は、第 1 のプロセス 1422 や第 2 のプロセス 1423 を管理する。

待避メモリ 1424 は、プロセス管理部 1421 の制御の下で、各種データを一時的に待避させるメモリである。

動作モード追加／削除指示部 1425 は、プロセス管理部 1421 の制御の下

で、CPU 1410における動作モード追加および削除を指示する。ファームウェアダウンロード/アンロード指示部1426は、プロセス管理部1421の制御の下でサーバ100（第36参照）からのファームウェアのダウンロード、およびファームウェア保持部316に設定されたファームウェアのアンロードを指示する。

コンテキストデータロード/アンロード指示部1427は、コンテキストデータ（CPU 1410内部のレジスタ（図示略）の値）のロードおよびアンロードを指示する。

つぎに、実施の形態7の動作について、第38図～第41図に示したフローチャートを参照しつつ説明する。第38図に示したステップSU1では、CPU 1410は、通常命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。

ステップSU2では、CPU 1410は、動作モード追加命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。ステップSU3では、CPU 1410は、ファームウェアダウンロード命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。

ステップSU4では、CPU 1410は、動作モード削除命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。この動作モード削除命令は、動作モード保持部312（第37図参照）に設定された動作モードを削除するための命令である。

ステップSU5では、CPU 1410は、ファームウェアアンロード命令が入力されたか否かを判断し、この場合、判断結果を「No」とする。このファームウェアアンロード命令は、ファームウェア保持部3-1-6に設定されたファームウェアをアンロードするための命令である。以後、CPU 1410は、ステップSU1～ステップSU5の判断を繰り返す。

そして、通常命令が入力されると、CPU 1410は、ステップSU1の判断結果を「Yes」とする。ステップSU6では、CPU 1410は、実施の形態

1と同様にして通常命令実行処理（第5図参照）を実行する。

ここで、動作モード（例えば、動作モード＝0）を追加するとともに、動作モード（例えば、動作モード＝1）を削除する場合、第41図に示したステップSX1では、第37図に示したオペレーティングシステム1420のプロセス管理部1421は、コンテキストデータロード／アンロード指示部1427に対して、第1のプロセス1422のコンテキストデータのアンロードを指示する。

ステップSX2では、コンテキストデータロード／アンロード指示部1427は、CPU1410から第1のプロセス1422のコンテキストデータをアンロードし、これをプロセス管理部1421経由で待避メモリ1424に待避する。

10 ステップSX3では、プロセス管理部1421は、ファームウェアダウンロード／アンロード指示部1426に対して、第1のプロセス1422の動作モード（動作モード＝1）に対応するファームウェアのアンロードを指示する。ステップSX4では、ファームウェアダウンロード／アンロード指示部1426は、CPU1410に対してファームウェアアンロード命令を発行する。

15 そして、上記ファームウェアアンロード命令が入力されると、CPU1410は、第38図に示したステップSU5の判断結果を「Yes」とする。ステップSU10では、CPU1410は、ファームウェアアンロード処理を実行する。

具体的には、第40図に示したステップSW1では、命令入力部311（第37図参照）は、命令バスを介して入力されたファームウェアアンロード命令を命令使用可否判断部314および命令実行部1411にフェッチする。ステップSW2では、動作モード保持部312は、現時点で設定されている動作モード＝1を使用可能命令保持部313へ通知する。

ステップSW3では、使用可能命令保持部313は、通知された動作モードに対応する使用可能命令群を命令使用可否判断部314へ通知する。

25 ステップSW4では、命令使用可否判断部314は、ステップSW1でフェッチされたファームウェアアンロード命令が、当該動作モードで使用可能であるか否かを判断する。この判断結果が「No」である場合、ステップSW7では、命

令使用可否判断部 3 1 4 は、権限違反または未定義命令例外割り込み発生（エラー）として処理する。

この場合、ステップ SW 4 の判断結果が「Y e s」であるとする、ステップ SW 5 では、命令実行部 1 4 1 1 は、ステップ SW 1 でフェッチされたファームウェアアンロード命令（使用可能命令）に対応する実行用のファームウェアをファームウェア保持部 3 1 6 から取得する。

ステップ SW 6 では、命令実行部 1 4 1 1 は、ファームウェアアンロード命令およびこれに対応する実行用のファームウェアに基づいて、ファームウェアアンロード命令に対応するファームウェアをファームウェア保持部 3 1 6 からアンロードし、これをデータ入出力部 3 1 7 を経由してファームウェアダウンロード／アンロード指示部 1 4 2 6 へ出力する。

第 4 1 図に戻り、ステップ SX 5 では、ファームウェアダウンロード／アンロード指示部 1 4 2 6 は、アンロードされたファームウェアをプロセス管理部 1 4 2 1 経由で待避メモリ 1 4 2 4 に待避する。ステップ SX 6 では、プロセス管理部 1 4 2 1 は、動作モード追加／削除指示部 1 4 2 5 に対して、第 1 のプロセス 1 4 2 2 の動作モード = 1 の削除を指示する。ステップ SX 7 では、動作モード追加／削除指示部 1 4 2 5 は、CPU 1 4 1 0 に対して、動作モード = 1 を削除するための動作モード削除命令を発行する。

そして、動作モード削除命令が入力されると、CPU 1 4 1 0 は、第 3 8 図に示したステップ SU 4 の判断結果を「Y e s」とする。ステップ SU 9 では、CPU 1 4 1 0 は、動作モード削除処理を実行する。

具体的には、第 3 9 図に示したステップ SV 1 では、命令入力部 3 1 1（第 3 7 図参照）は、命令バスを介して入力された動作モード削除命令を命令使用可否判断部 3 1 4 および命令実行部 1 4 1 1 にフェッチする。

ステップ SV 2 では、動作モード保持部 3 1 2 は、現時点で設定されている動作モードを使用可能命令保持部 3 1 3 へ通知する。

ステップ SV 3 では、使用可能命令保持部 3 1 3 は、通知された動作モードに

対応する使用可能命令群を命令使用可否判断部 3 1 4 へ通知する。

ステップ S V 4 では、命令使用可否判断部 3 1 4 は、ステップ S V 1 でフェッチされた動作モード削除命令が、当該動作モードで使用可能であるか否かを判断する。この判断結果が「N o」である場合、ステップ S V 7 では、命令使用可否
5 判断部 3 1 4 は、権限違反または未定義命令割り込み発生（エラー）として処理する。

この場合、ステップ S V 4 の判断結果が「Y e s」であるとする、ステップ S V 5 では、命令実行部 1 4 1 1 は、ステップ S V 1 でフェッチされた動作モード削除命令（使用可能命令）に対応するファームウェアをファームウェア保持部
10 3 1 6 から取得する。

ステップ S V 6 では、命令実行部 1 4 1 1 は、動作モード保持部 3 1 2 に設定されている動作モードのうち動作モード追加／削除指示部 1 4 2 5 により指示された動作モードを削除する。

第 4 1 図に戻り、ステップ S X 8 では、プロセス管理部 1 4 2 1 は、動作モード追加／削除指示部 1 4 2 5 に対して、第 2 のプロセス 1 4 2 3 の動作モード＝
15 0 の追加を指示する。ステップ S X 9 では、動作モード追加／削除指示部 1 4 2 5 は、C P U 1 4 1 0 に対して、動作モード＝0 を追加するための動作モード追加命令を発行する。

そして、動作モード追加命令が入力されると、C P U 1 4 1 0 は、第 3 8 図に示したステップ S U 2 の判断結果を「Y e s」とする。ステップ S U 7 では、C
20 P U 1 4 1 0 は、実施の形態 1 と同様にして動作モード追加処理（第 6 図参照）を実行する。これにより、動作モード保持部 3 1 2 には、動作モード＝0 が追加される。

第 4 1 図に戻り、ステップ S X 1 0 では、プロセス管理部 1 4 2 1 は、ファームウェアダウンロード／アンロード指示部 1 4 2 6 に対して、第 2 のプロセス 1
25 4 2 3 の動作モード（動作モード＝0）に対応するファームウェアのダウンロードロードを指示する。ステップ S X 1 1 では、ファームウェアダウンロード／ア

ンロード指示部 1 4 2 6 は、CPU 1 4 1 0 に対してファームウェアダウンロード命令を発行する。

そして、上記ファームウェアダウンロード命令が入力されると、CPU 1 4 1 0 は、第 3 8 図に示したステップ S U 3 の判断結果を「Y e s」とする。ステップ S U 8 では、CPU 1 4 1 0 は、実施の形態 1 と同様にしてファームウェアダウンロード処理（第 7 図参照）を実行する。これにより、ファームウェア保持部 3 1 6 には、動作モード＝0 に対応するファームウェアが設定される。

第 4 1 図に戻り、ステップ S X 1 2 では、第 3 7 図に示したオペレーティングシステム 1 4 2 0 のプロセス管理部 1 4 2 1 は、コンテキストデータロード／アンロード指示部 1 4 2 7 に対して、第 2 のプロセス 1 4 2 3 のコンテキストデータのロードを指示する。ステップ S X 1 3 では、コンテキストデータロード／アンロード指示部 1 4 2 7 は、第 2 のプロセス 1 4 2 3 のコンテキストデータを CPU 1 4 1 0 にロードする。

以上説明したように、実施の形態 7 によれば、複数の動作モードのうち動的に指定された動作モードを動作モード保持部 3 1 2 （第 3 7 図参照）から削除し、さらに削除された動作モードに対応するファームウェアをファームウェア保持部 3 1 6 から削除するようにしたので、有限である CPU 1 4 1 0 の資源を有効に活用することができる。

（実施の形態 8）

さて、前述した実施の形態 1 では、ステップ S B 9 （第 5 図参照）、ステップ S C 8 （第 6 図参照）またはステップ S D 8 （第 7 図参照）で未定義命令例外割り込み発生（エラー）の場合、通常命令実行処理、動作モード追加処理またはファームウェアダウンロード処理を中断する例について説明したが、CPU 3 1 0 （第 2 図参照）の外部に、CPU 3 1 0 における各種処理をエミュレートするエミュレート部を設ける構成としてもよい。以下では、この構成例を実施の形態 8 として説明する。

第 4 2 図は、本発明にかかる実施の形態 8 の構成を示すブロック図である。こ

の図において、第1図の各部に対応する部分には同一の符号を付け、その説明を省略する。

クライアント1500は、インターネット200に接続されており、インターネット200を介して、サーバ100からファームウェアをダウンロードする機能と、ファームウェアを用いて各種命令を実行し、結果を出力する機能と、エミューレート機能とを備えている。

クライアント1500において、CPU1510は、ファームウェアを動的にダウンロードさせるための制御や、後述する動作モードや命令群の設定等を行う。エミューレート部1520は、CPU1510で未定義命令例外割り込み発生（エラー）の場合、通常命令実行処理、動作モード追加処理またはファームウェアダウンロード処理をエミューレートする。

第43図は、第42図に示したCPU1510およびエミューレート部1520の構成を示すブロック図である。この図において、第2図の各部に対応する部分には同一の符号を付け、その説明を省略する。

命令実行部1511は、命令使用可否判断部314により使用可能と判断された命令の実行に用いられるファームウェアをファームウェア保持部316より取得し、当該命令を実行する。また、命令実行部1511は、命令実行時に未定義命令例外割り込み（エラー）が発生した場合、エミューレート部1520のアドレスにジャンプし、エミューレート部1520に当該命令に対応する処理をエミューレートさせる。

エミューレート部1520において、制御部1521は、各部を制御する。動作モード保持部1522は、動作モード保持部312と同一の機能を備えており、動作モードを保持する。使用可能命令保持部1523は、使用可能命令保持部313と同一の機能を備えており、動作モード保持部1522に設定された動作モードに対応する使用可能命令を保持する。

ジャンプ先アドレス格納部1524は、未定義命令例外割り込み発生（エラー）の場合のジャンプ先アドレスを格納している。未定義命令割り込みハンドラ

1 5 2 5 は、命令実行部 1 5 1 1 と同一の機能を備えており、未定義命令例外割り込み発生（エラー）の場合に命令実行部 1 5 1 1 での処理をエミュレートする。

つぎに、実施の形態 8 の動作について、第 5 図～第 7 図および第 4 4 図に示したフローチャートを参照しつつ説明する。

- 5 第 4 4 図に示したステップ S Y 1 では、命令実行部 1 5 1 1 は、第 5 図、第 6 図または第 7 図に示した通常命令実行処理、動作モード追加処理またはファームウェアダウンロード処理で未定義命令例外割り込み（エラー）が発生したか否かを判断し、この場合、判断結果を「N o」として、同判断を繰り返す。

- 10 例えば、第 5 図に示したステップ S B 9 で未定義命令例外割り込みが発生すると、命令実行部 1 5 1 1 は、第 4 4 図に示したステップ S Y 1 の判断結果を「Y e s」とする。ステップ S Y 2 では、命令実行部 1 5 1 1 は、ジャンプ先アドレスにジャンプし、未定義命令割り込みハンドラ 1 5 2 5 に当該命令（この場合、通常命令）および動作モードを通知する。ステップ S Y 3 では、未定義命令割り込みハンドラ 1 5 2 5 は、未定義命令割り込みハンドラの実行を開始する。

- 15 ステップ S Y 4 では、未定義命令割り込みハンドラ 1 5 2 5 は、命令実行部 1 5 1 1 より通知された当該命令の種別を判断する。ステップ S Y 5 では、未定義命令割り込みハンドラ 1 5 2 5 は、当該命令（この場合、通常命令）が使用可能であるか否かを判断する。

- 20 具体的には、未定義命令割り込みハンドラ 1 5 2 5 は、命令実行部 1 5 1 1 より通知された動作モードに対応する使用可能命令群を使用可能命令保持部 1 5 2 3 から取得し、この使用可能命令群に当該命令（この場合通常命令）が存在するか否かを判断し、この場合、判断結果を「Y e s」とする。

- 25 ステップ S Y 6 では、未定義命令割り込みハンドラ 1 5 2 5 は、当該命令（この場合、通常命令）の実行をエミュレートするエミュレート処理を実行する。具体的には、未定義命令割り込みハンドラ 1 5 2 5 は、当該命令（この場合、通常命令）に対応するファームウェアをファームウェア保持部 3 1 6 から取得する。

つぎに、未定義命令割り込みハンドラ 1 5 2 5 は、データバスより命令実行に

用いられるデータを取得した後、ファームウェアおよびデータを用いて通常命令を実行する。つぎに、未定義命令割り込みハンドラ 1525 は、通常命令を実行した結果をデータバスへ出力する。

一方、ステップ SY5 の判断結果が「No」である場合、すなわち、ステップ 5 SY7 では、未定義命令割り込みハンドラ 1525 は、権限違反例外割り込み通知を命令実行部 1511 へ出す。

以上説明したように、実施の形態 8 によれば、動作モード保持部 312（第 4 3 図参照）に保持された動作モードに対応する命令に関して未定義命令例外割り込み（エラー）が発生した場合、当該命令の実行を外部のエミュレート部 152 10 0 に依頼するようにしたので、命令実行の信頼性を高めることができる。

以上本発明にかかる実施の形態 1～8 について図面を参照して詳述してきたが、具体的な構成例はこれらの実施の形態 1～8 に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。

例えば、前述した実施の形態 1～8 においては、前述した各種機能を実現する 15 ためのプログラムを第 45 図に示したコンピュータ読み取り可能な記録媒体 1700 に記録して、この記録媒体 1700 に記録されたプログラムを同図に示したコンピュータ 1600 に読み込ませ、実行することにより各種機能を実現してもよい。

同図に示したコンピュータ 1600 は、上記プログラムを実行する CPU 16 20 10 と、キーボード、マウス等の入力装置 1620 と、各種データを記憶する ROM 1630 と、演算パラメータ等を記憶する RAM 1640 と、記録媒体 1700 からプログラムを読み取る読取装置 1650 と、ディスプレイ、プリンタ等の出力装置 1660 と、装置各部を接続するバス 1670 とから構成されている。

CPU 1610 は、読取装置 1650 を経由して記録媒体 1700 に記録され 25 ているプログラムを読み込んだ後、このプログラムを実行することにより、前述した各種機能を実現する。なお、記録媒体 1700 には、光ディスク、フレキシブルディスク、ハードディスク等の可搬型の記録媒体が含まれることはもとより、

ネットワークのようにデータを一時的に記録保持するような伝送媒体も含まれる。

また、実施の形態1～8においては、それぞれの特徴を組み合わせて構成してもよい。組み合わせの構成も本発明に含まれる。

5 以上説明したように、本発明によれば、複数の動作モードのうち動的に指定された動作モードを動作モード保持手段に追加し、追加された動作モードに対応する命令を使用可能命令保持手段に設定し、さらに、命令の実行に用いられるファームウェアを外部から取得するようにしたので、セキュリティを維持しつつ拡張性を高めることができ、コストを低減させることができるという効果を奏する。

10 また、本発明によれば、暗号化されたファームウェアを外部から取得した後、該ファームウェアを復号するようにしたので、ファームウェア取得中のセキュリティを高めることができるという効果を奏する。

また、本発明によれば、電子署名付きのファームウェアを外部から取得した後、該ファームウェアを認証するようにしたので、ファームウェア取得中の改竄等を防止することができるという効果を奏する。

15 また、本発明によれば、動作モードに応じて、命令の実行に際して利用される各種資源に対するアクセス制御を行うようにしたので、動作モードに応じて動的に資源を割り当てることができるという効果を奏する。

20 また、本発明によれば、動的に指定された動作モードの命令数が、動作モード保持手段に既に保持されている動作モードの命令数より多い場合に限り、動的に指定された動作モードを動作モード保持手段に追加するようにしたので、より厳しい条件での動作モードの追加が可能となり、セキュリティをさらに高めることができるという効果を奏する。

25 また、本発明によれば、複数の動作モードのうち動的に指定された動作モードを動作モード保持手段から削除し、さらに削除された動作モードに対応するファームウェアを削除するようにしたので、有限である中央演算装置の資源を有効に活用することができるという効果を奏する。

また、本発明によれば、動作モード保持手段に保持された動作モードに対応す

る命令に関してエラーが発生した場合、当該命令の実行を外部のエミュレータに依頼するようにしたので、命令実行の信頼性を高めることができるという効果を奏する。

5 また、本発明によれば、複数の動作モードのうち動的に指定された動作モードを動作モード保持手段に追加し、追加された動作モードに対応する命令を使用可能命令保持手段に設定し、さらに、動作モード保持手段に保持された動作モードに対応し、命令の実行に用いられる論理回路を生成するための論理回路データを外部から取得するようにしたので、セキュリティを維持しつつ拡張性を高めることができ、コストを低減させることができるという効果を奏する。

10 また、本発明によれば、命令の実行に際して、該命令に対応する論理回路データに基づいて、動的に論理回路を生成するようにしたので、セキュリティを維持しつつ拡張性を高めることができ、コストを低減させることができるという効果を奏する。

15 産業上の利用可能性

以上のように、本発明にかかる中央演算装置および演算プログラムは、暗号化／復号、電子署名等のセキュリティ機能を提供するサーバ、クライアントに対して有用である。

請 求 の 範 囲

1. 複数の動作モードのうち単数または複数の動作モードを保持する動作モード保持手段と、

- 5 前記動作モード保持手段により保持された動作モードに対応する命令を、使用可能命令として保持する使用可能命令保持手段と、

前記複数の動作モードのうち動的に指定された動作モードを前記動作モード保持手段に追加し、追加された動作モードに対応する命令を前記使用可能命令保持手段に設定する動作モード追加手段と、

- 10 前記動作モード保持手段に保持された動作モードに対応し、命令の実行に用いられるファームウェアを外部から取得するファームウェア取得手段と、
を備えたことを特徴とする中央演算装置。

2. 前記ファームウェア取得手段は、暗号化されたファームウェアを外部から取得した後、該ファームウェアを復号することを特徴とする請求の範囲第1項に記載の中央演算装置。

3. 前記ファームウェア取得手段は、電子署名付きのファームウェアを外部から取得した後、該ファームウェアを認証することを特徴とする請求の範囲第1項に記載の中央演算装置。

4. 前記動作モードに応じて、命令の実行に際して利用される各種資源に対するアクセス制御を行うアクセス制御手段を備えたことを特徴とする請求の範囲第1項～第3項のいずれか一つに記載の中央演算装置。

5. 前記動作モード追加手段は、前記動的に指定された動作モードの命令数が、動作モード保持手段に既に保持されている動作モードの命令数より多い場合に限

り、前記動的に指定された動作モードを前記動作モード保持手段に追加し、追加された動作モードに対応する命令を前記使用可能命令保持手段に設定することを特徴とする請求の範囲第1項～第3項のいずれか一つに記載の中央演算装置。

- 5 6. 前記複数の動作モードのうち動的に指定された動作モードを前記動作モード保持手段から削除する動作モード削除手段と、前記削除された動作モードに対応するファームウェアを削除するファームウェア削除手段とを備えたことを特徴とする請求の範囲第1項～第3項のいずれか一つに記載の中央演算装置。

- 10 7. 前記動作モード保持手段に保持された動作モードに対応する命令に関してエラーが発生した場合、当該命令の実行を外部のエミュレータに依頼する実行依頼手段を備えたことを特徴とする請求の範囲第1項～第3項のいずれか一つに記載の中央演算装置。

- 15 8. 複数の動作モードのうち単数または複数の動作モードを保持する動作モード保持手段と、

前記動作モード保持手段により保持された動作モードに対応する命令を、使用可能命令として保持する使用可能命令保持手段と、

- 20 前記複数の動作モードのうち動的に指定された動作モードを前記動作モード保持手段に追加し、追加された動作モードに対応する命令を前記使用可能命令保持手段に設定する動作モード追加手段と、

前記動作モード保持手段に保持された動作モードに対応し、命令の実行に用いられる論理回路を生成するための論理回路データを外部から取得する論理回路データ取得手段と、

- 25 を備えたことを特徴とする中央演算装置。

9. 前記命令の実行に際して、該命令に対応する論理回路データに基づいて、動

的に論理回路を生成する論理回路生成手段を備えたことを特徴とする請求の範囲第8項に記載の中央演算装置。

10. コンピュータを、

- 5 複数の動作モードのうち単数または複数の動作モードを保持する動作モード保持手段、

前記動作モード保持手段により保持された動作モードに対応する命令を、使用可能命令として保持する使用可能命令保持手段、

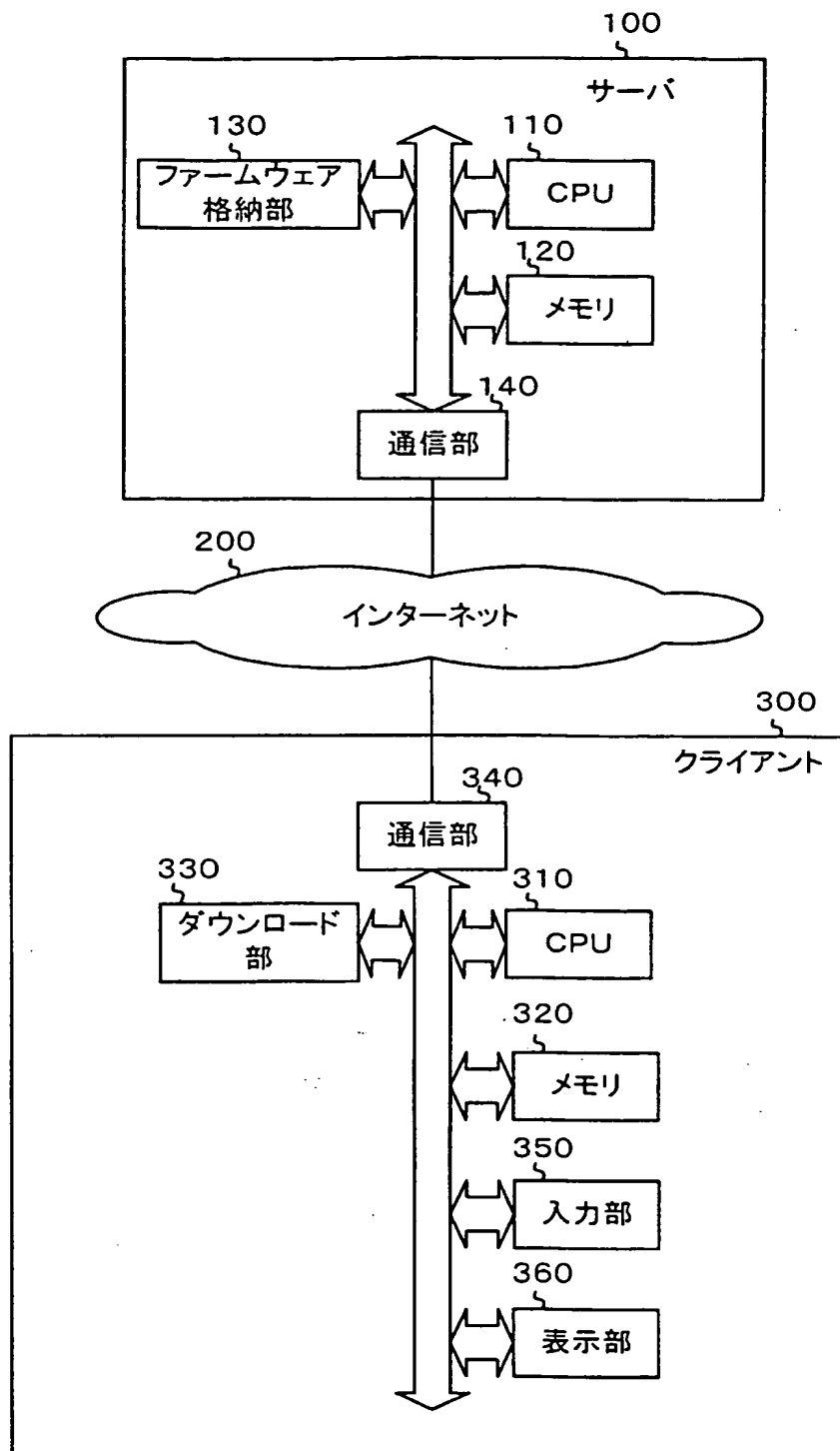
- 10 前記複数の動作モードのうち動的に指定された動作モードを前記動作モード保持手段に追加し、追加された動作モードに対応する命令を前記使用可能命令保持手段に設定する動作モード追加手段、

前記動作モード保持手段に保持された動作モードに対応し、命令の実行に用いられるファームウェアを外部から取得するファームウェア取得手段、

として機能させるための演算プログラム。

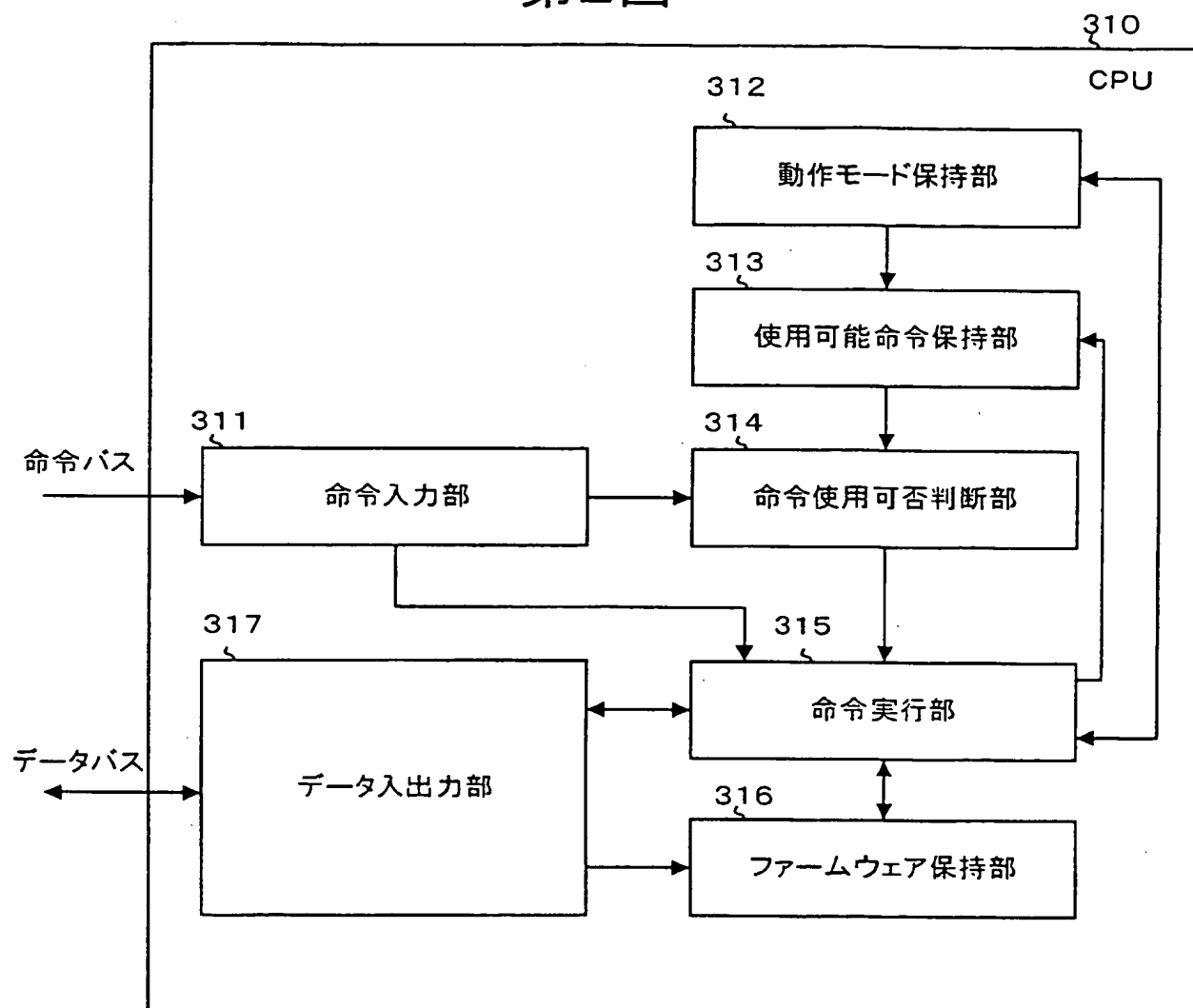
1/46

第1図



THIS PAGE BLANK (USPTO)

第2図



THIS PAGE BLANK (USPTO)

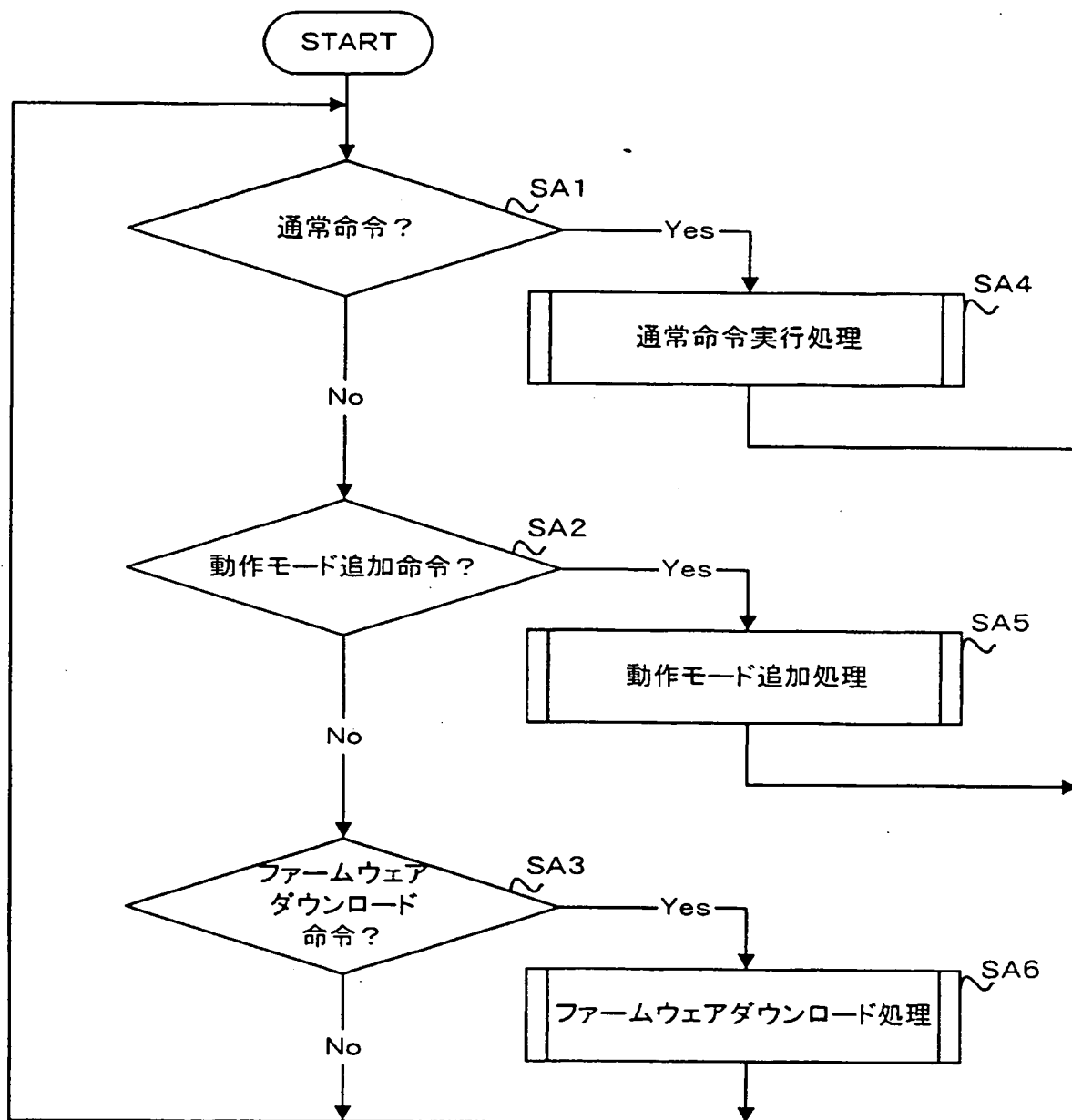
第3図

400

動作モード	使用可能命令数	命令1	命令2	命令i	命令n
0	n	0x01	0x13	0xf2	0xf8
1	i	0x11	0x23	0xe7	—	—
:	:	:	:	:	:	:	:
k	1	0xff	—	—	—	—	—

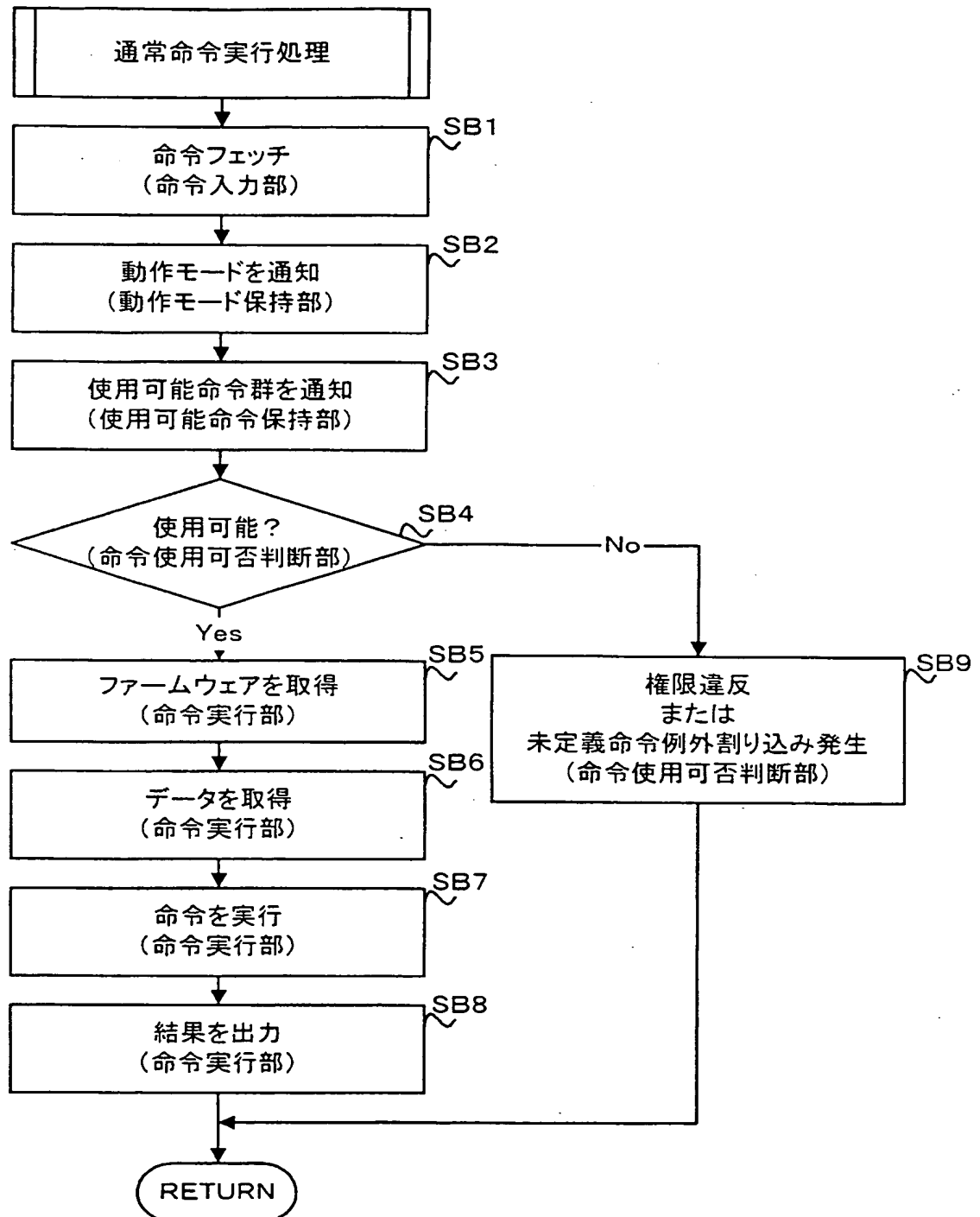
THIS PAGE BLANK (USPTO)

第4図



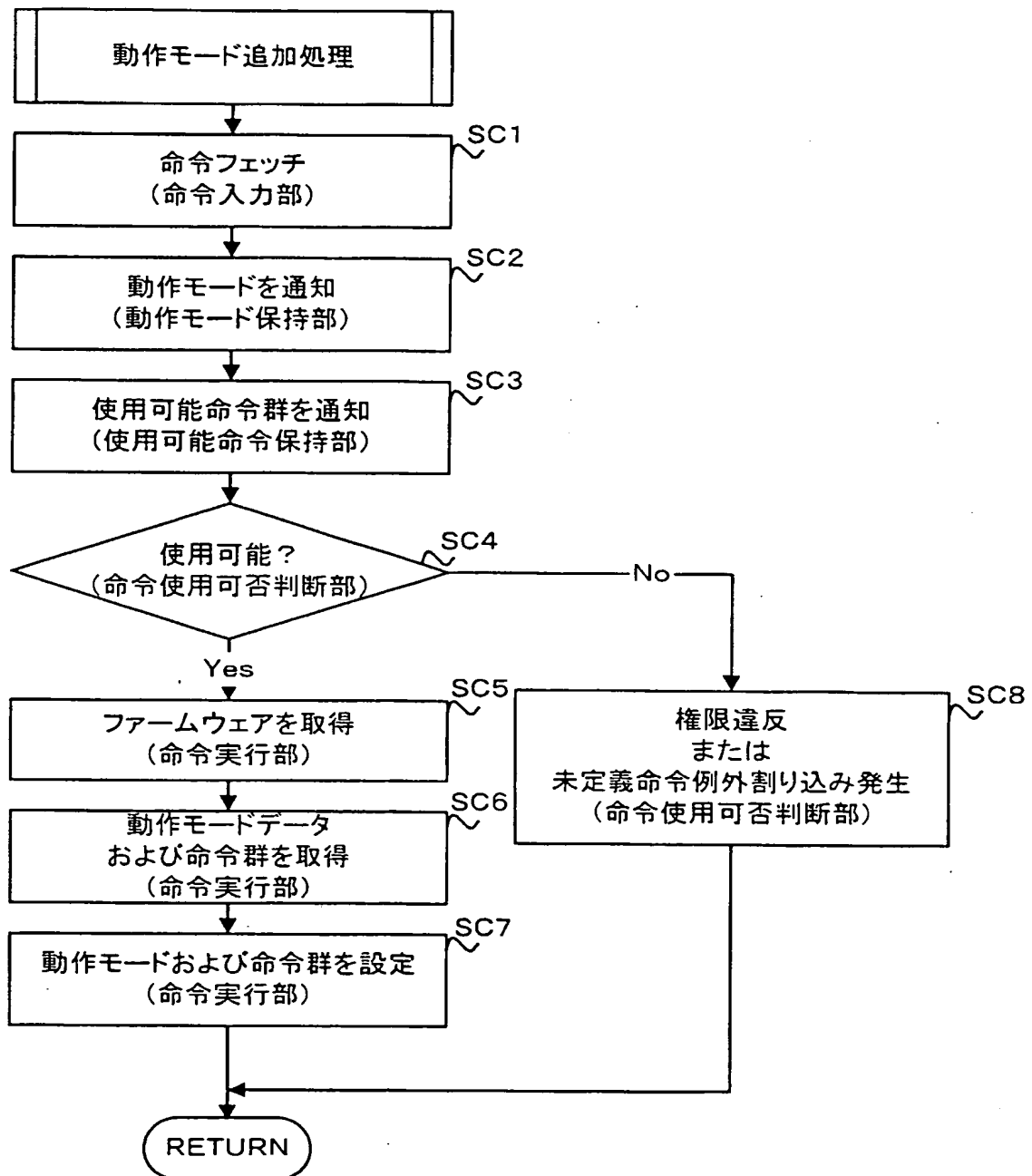
THIS PAGE BLANK (USPTO)

第5図



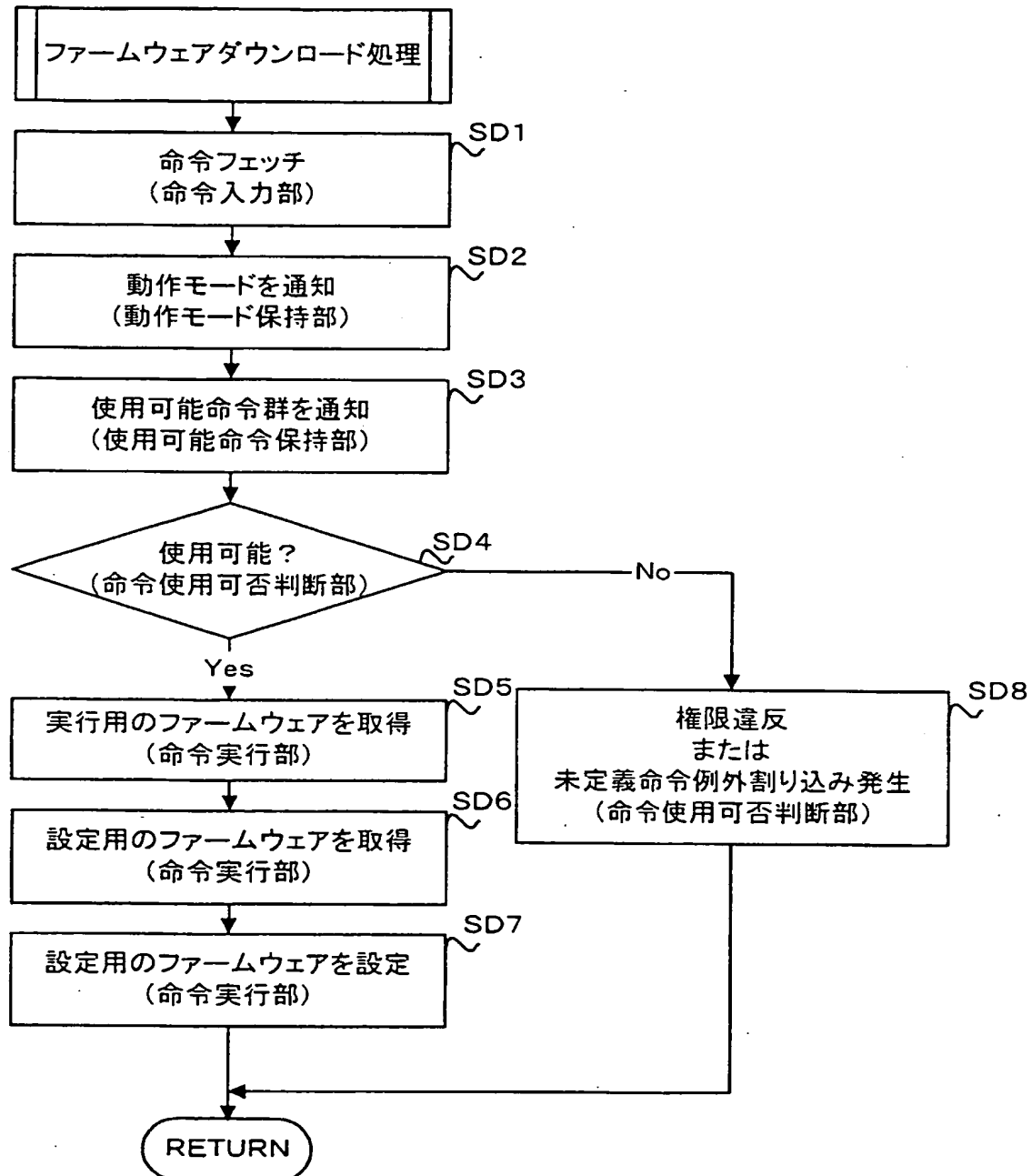
THIS PAGE BLANK (USPTO)

第6図



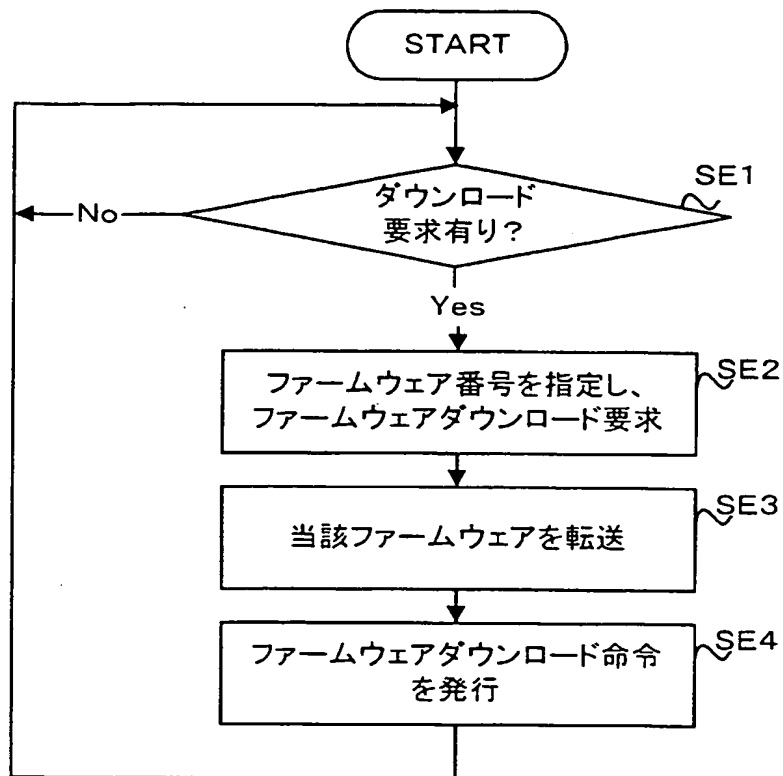
THIS PAGE BLANK (USPTO)

第7図



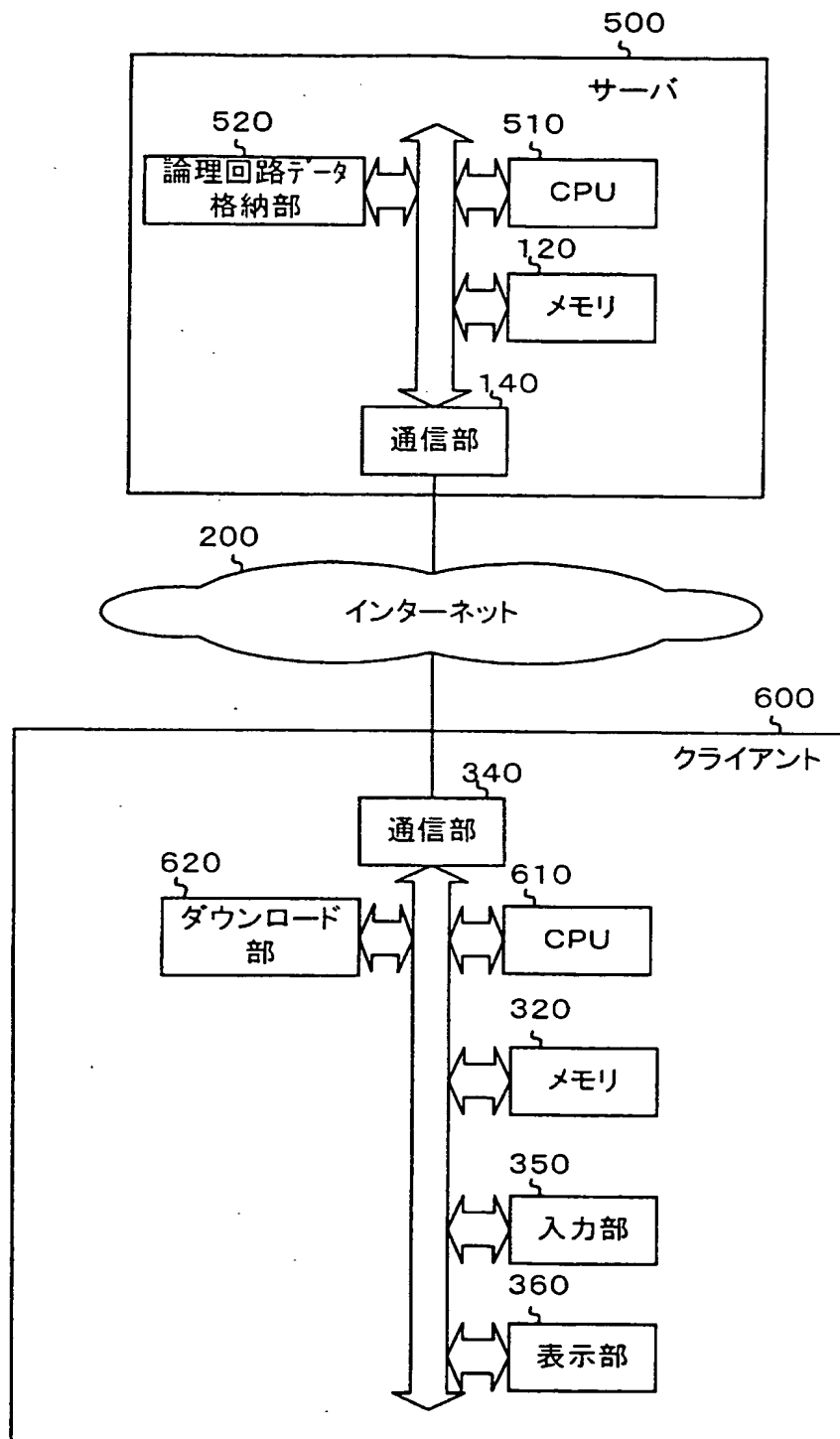
THIS PAGE BLANK (USPTO)

第8図



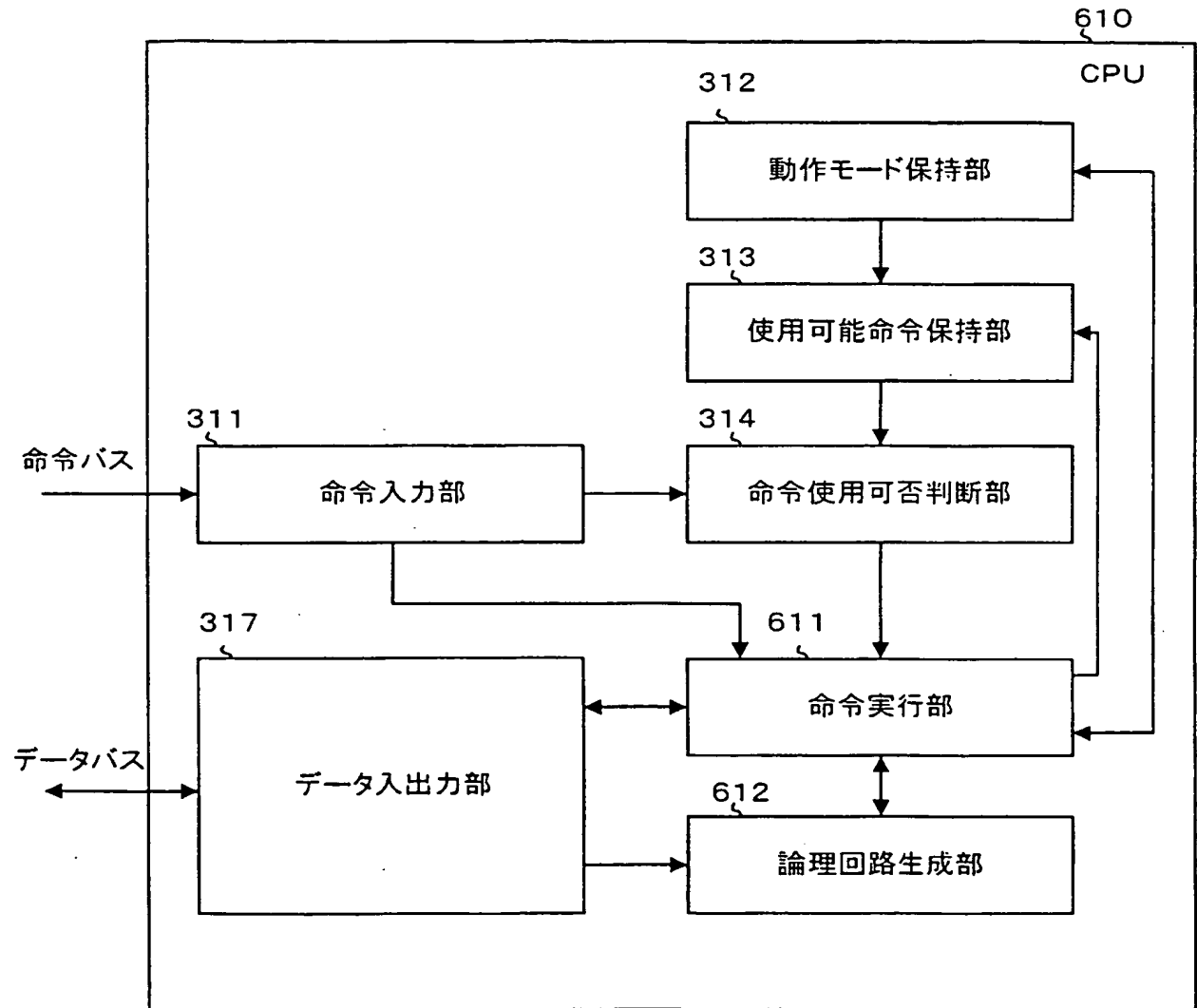
THIS PAGE BLANK (USPTO)

第9図



THIS PAGE BLANK (USPTO)

第10図



THIS PAGE BLANK (USPTO)

This page is not part of
the document!

JP2001010446 / 2003-046715

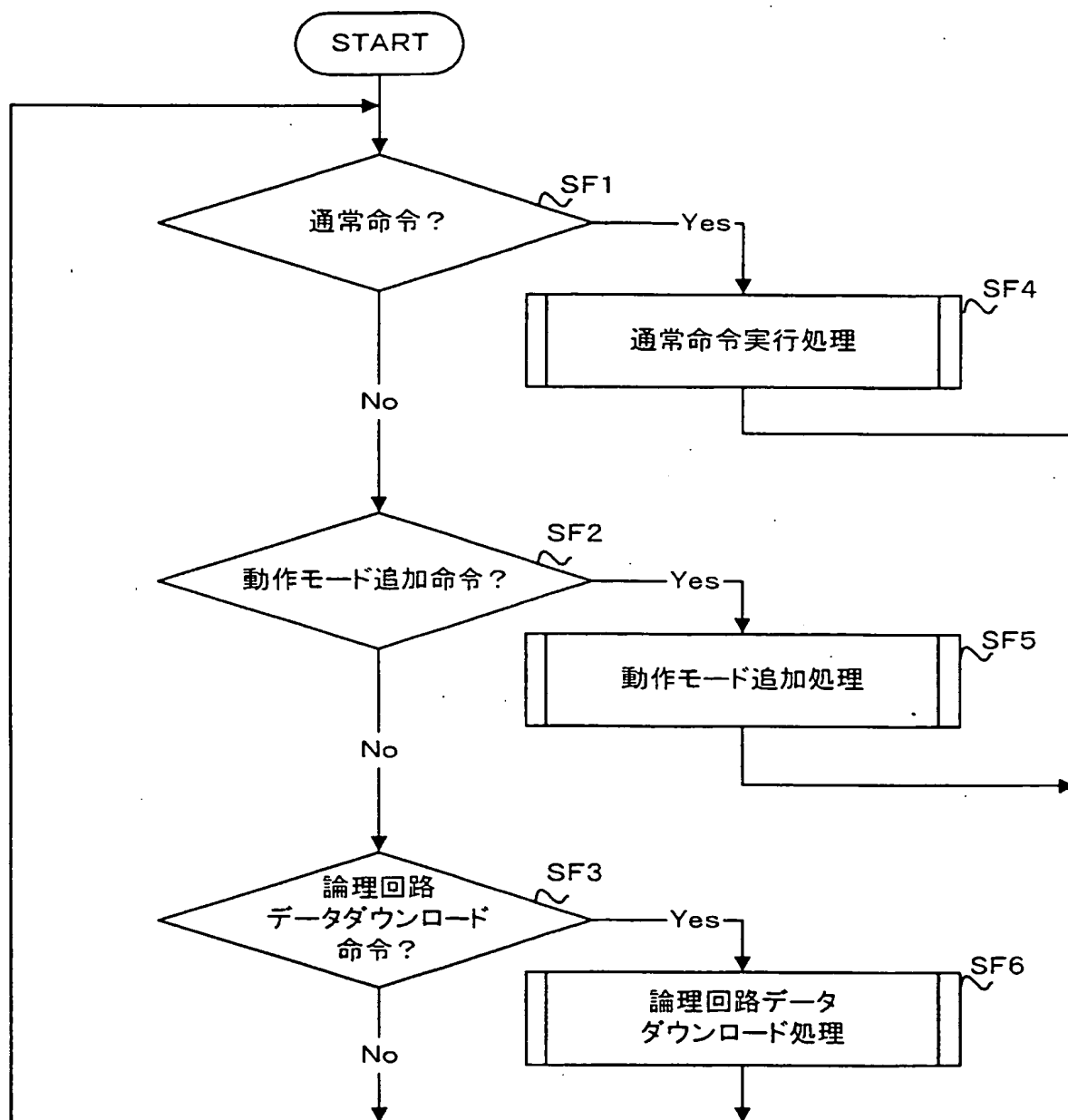
2/2

Date: Jun 5, 2003

Recipient: IB

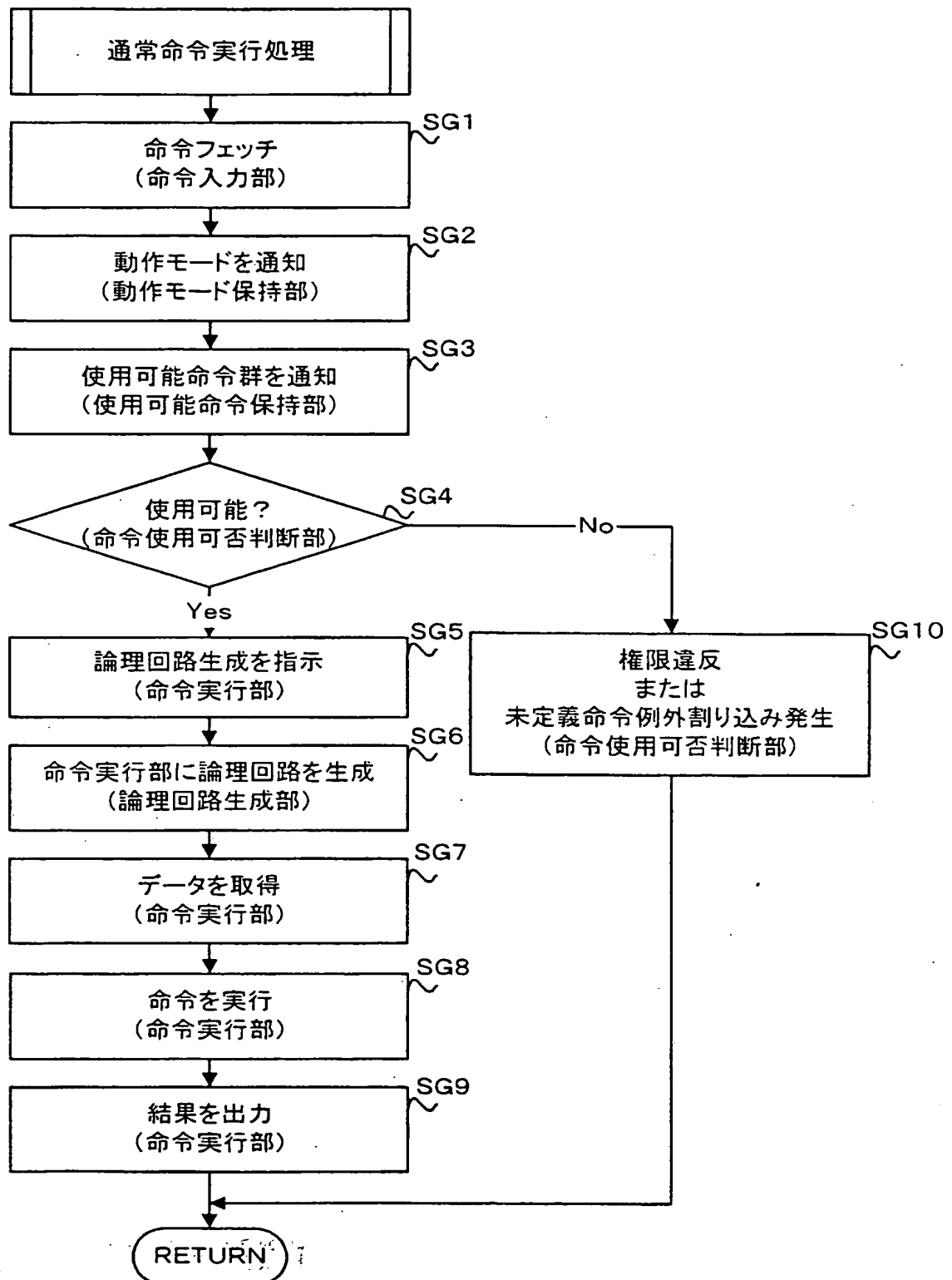
THIS PAGE BLANK (USPTO)

第11図



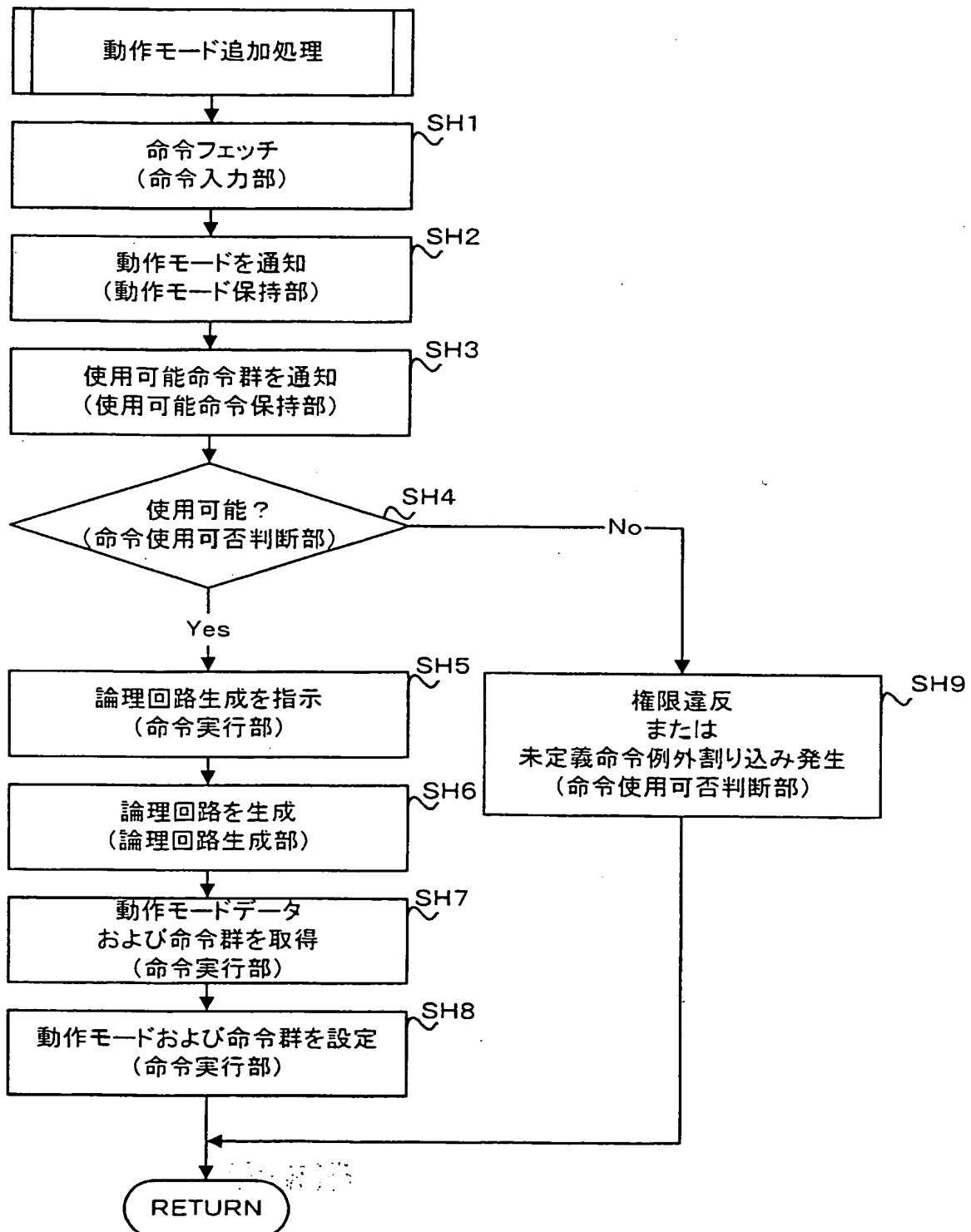
THIS PAGE BLANK (USPTO)

第12図



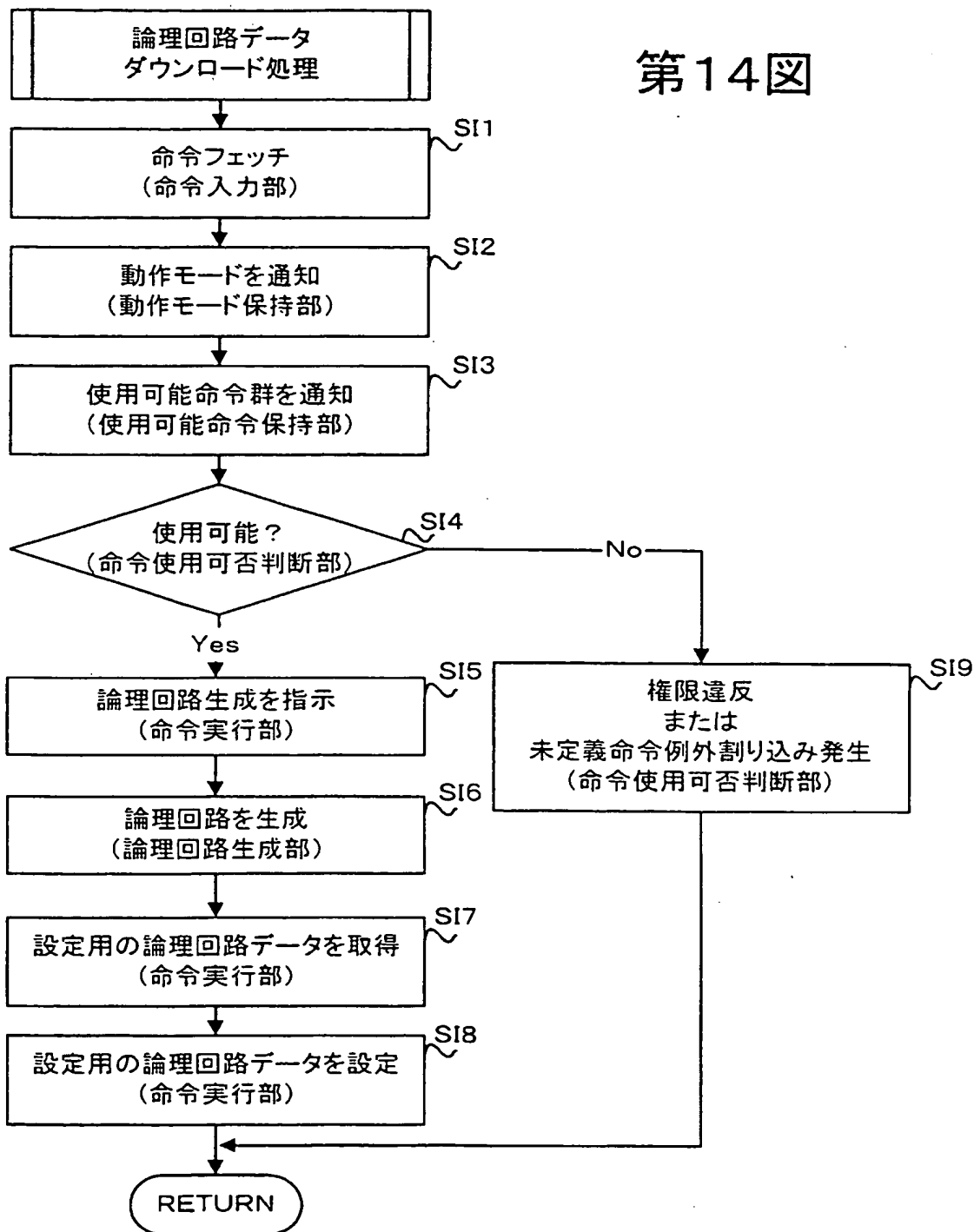
THIS PAGE BLANK (USPTO)

第13図



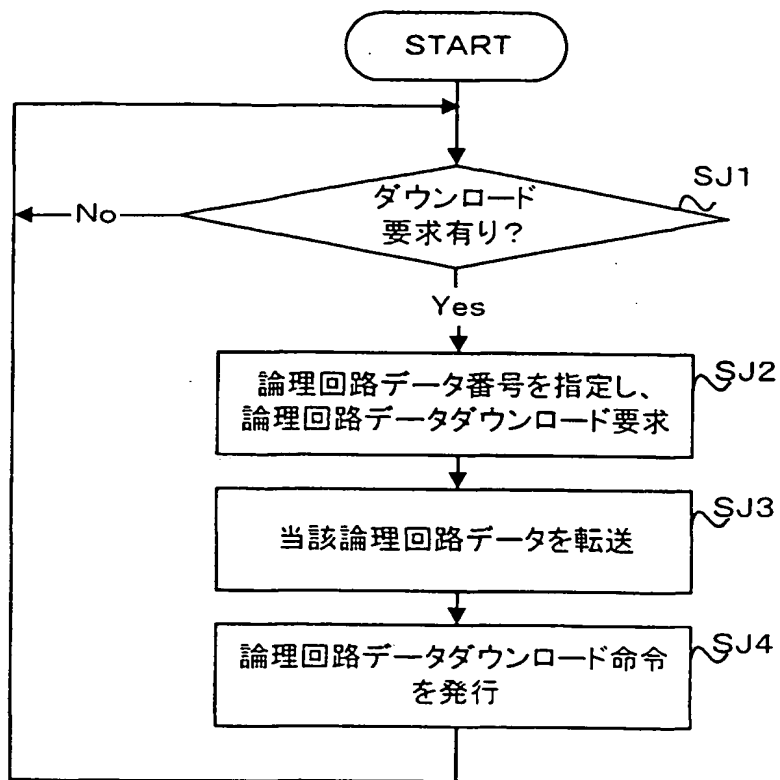
THIS PAGE BLANK (USPTO)

第14図



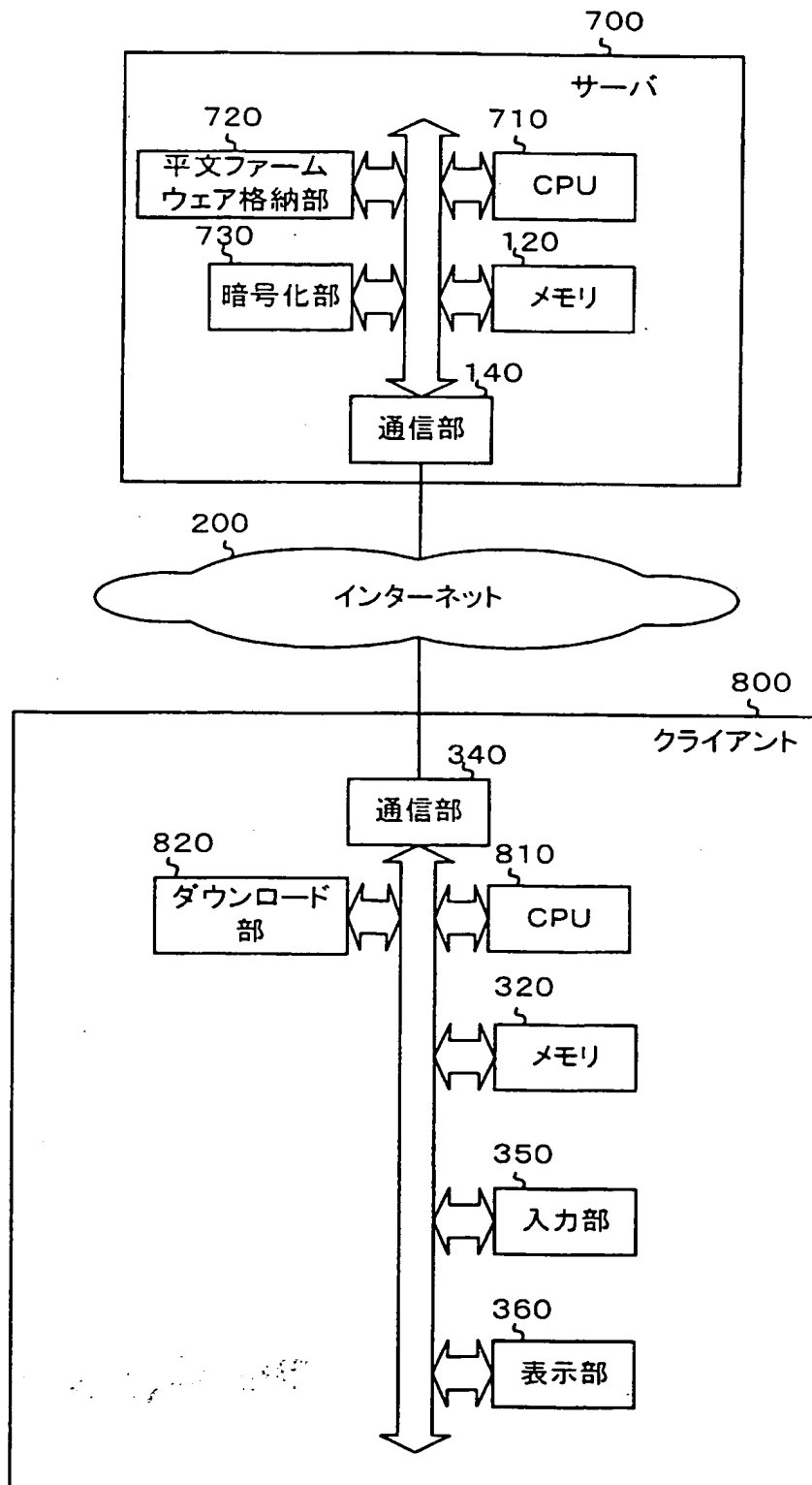
THIS PAGE BLANK (USPTO)

第15図



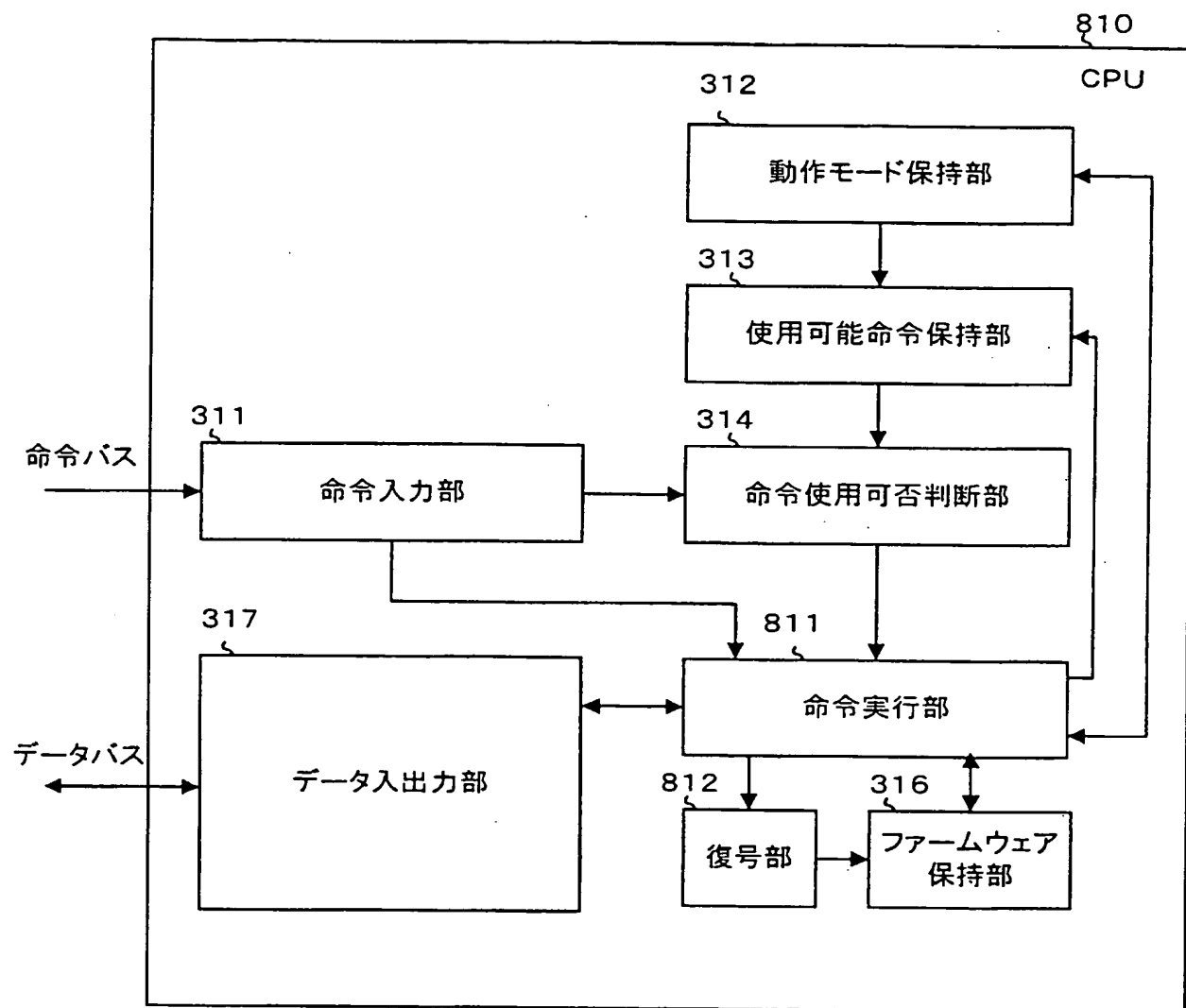
THIS PAGE BLANK (USPTO)

第16図



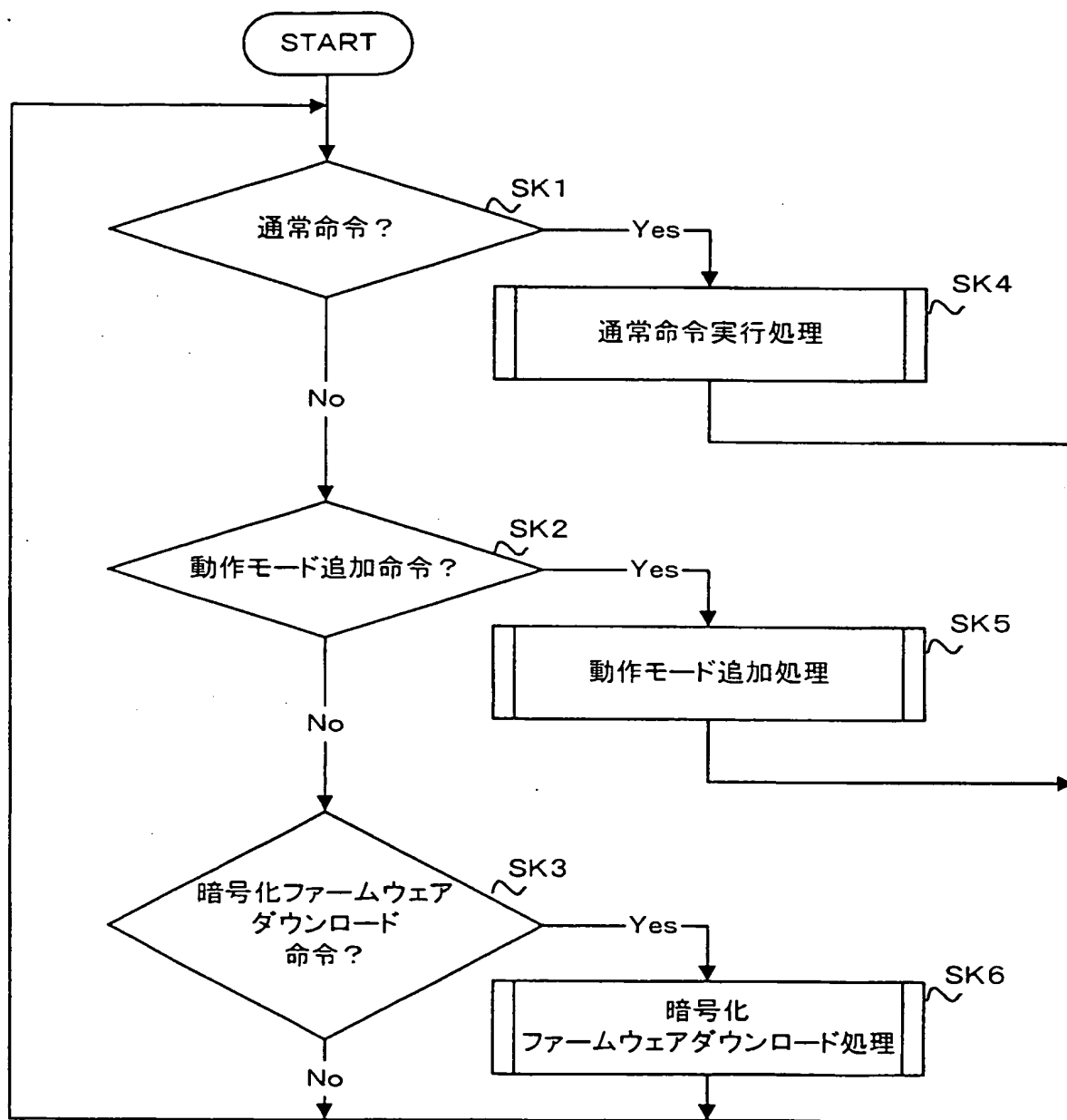
THIS PAGE BLANK (USPTO)

第17図



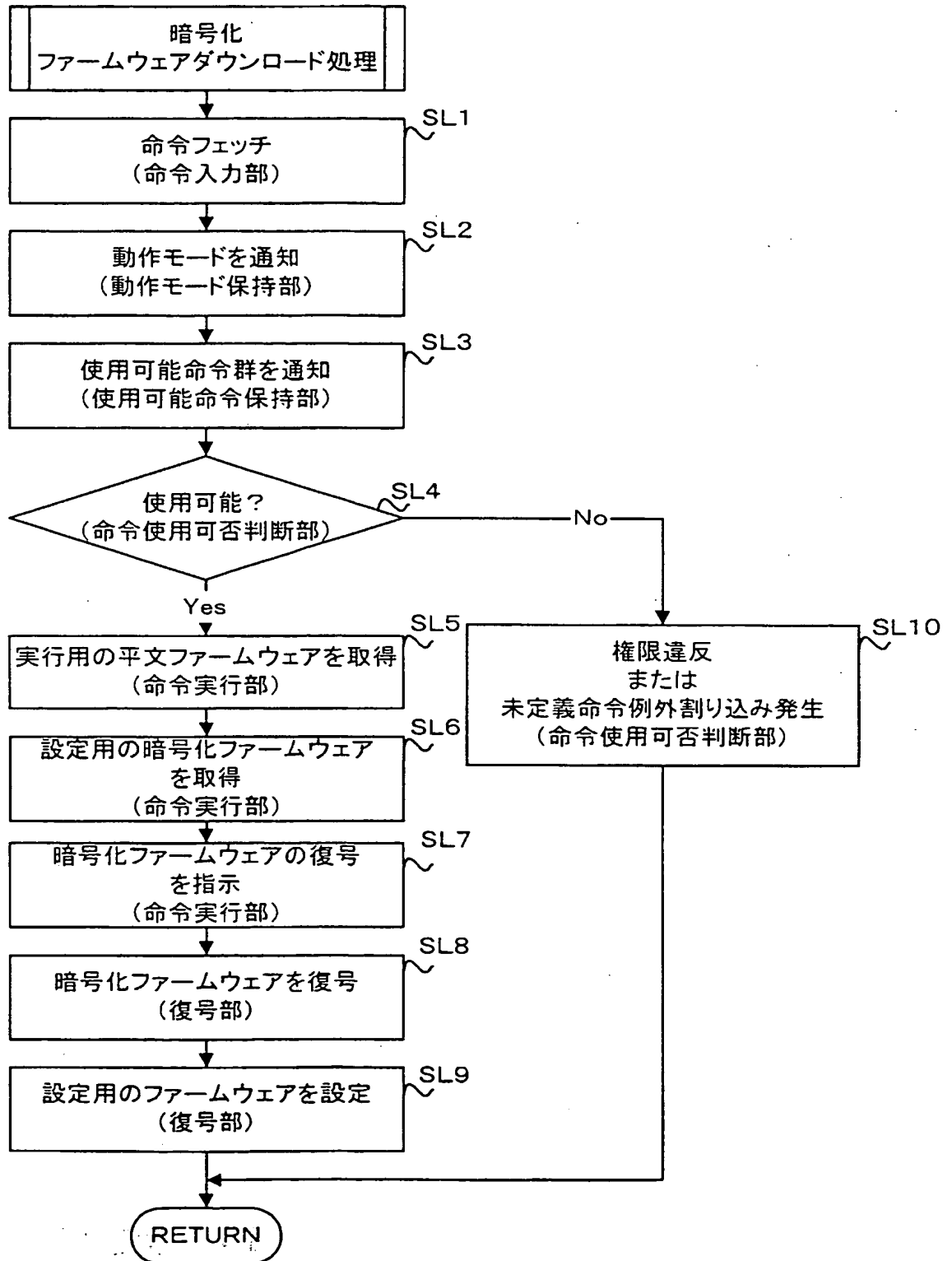
THIS PAGE BLANK (USPTO)

第18図



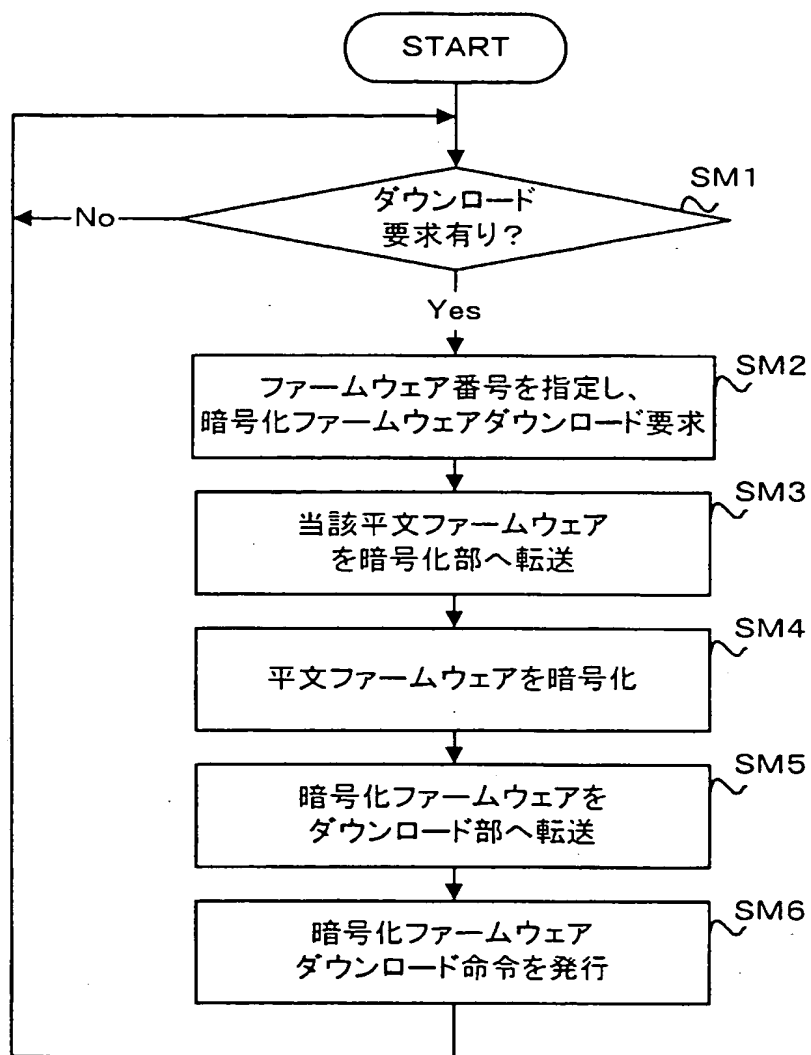
THIS PAGE BLANK (USPTO)

第19図



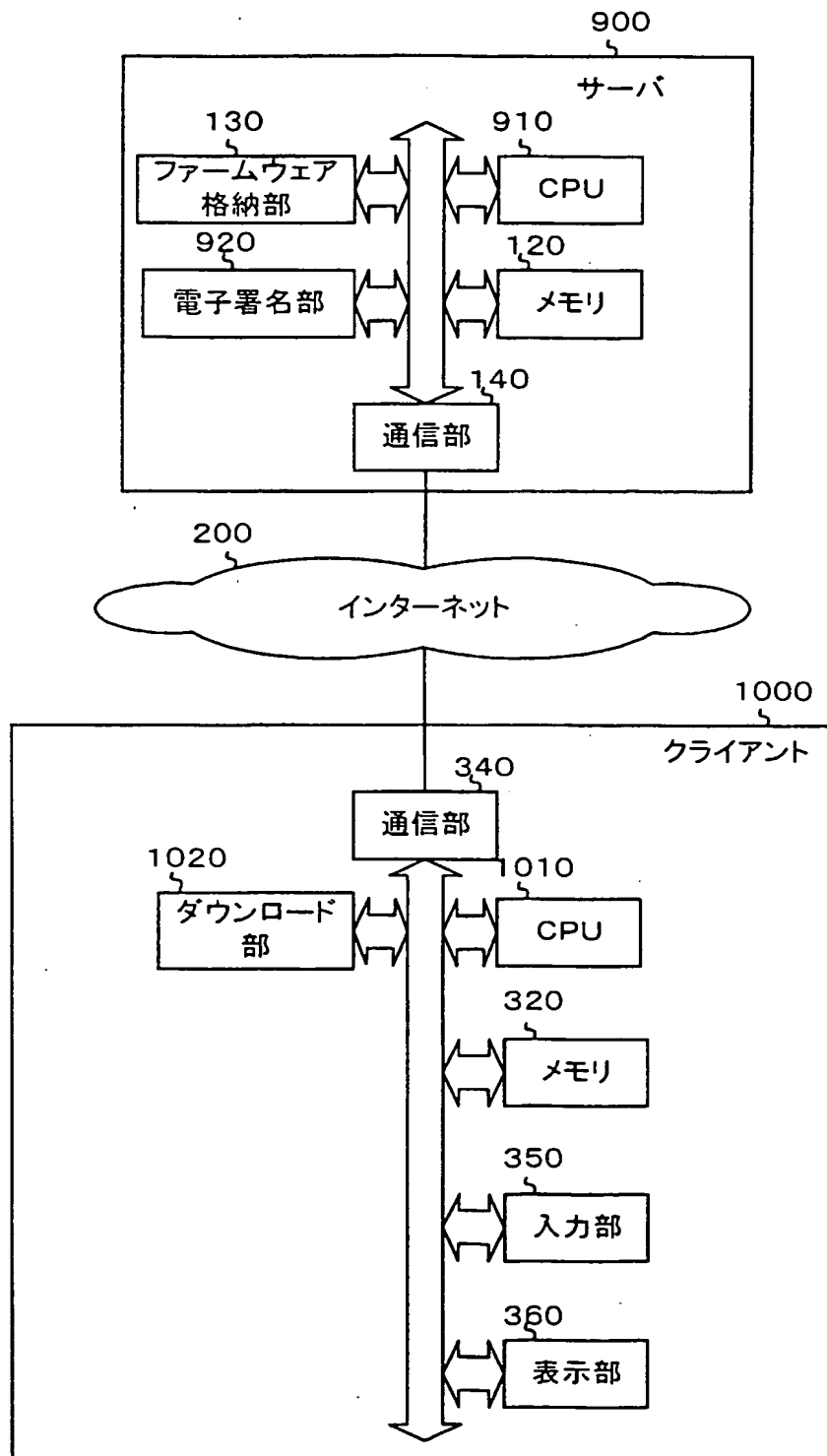
THIS PAGE BLANK (USPTO)

第20図



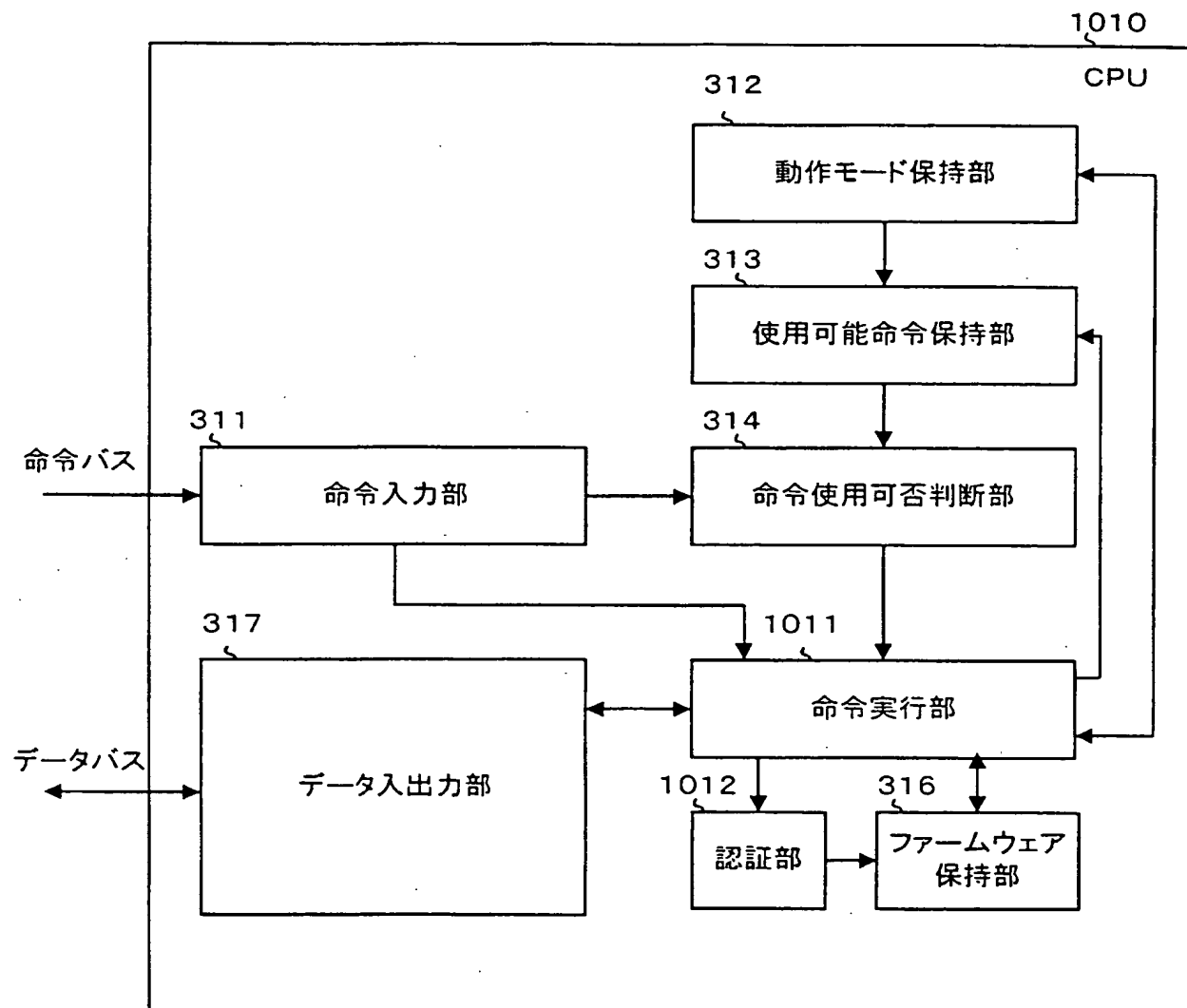
THIS PAGE BLANK (USPTO)

第21図



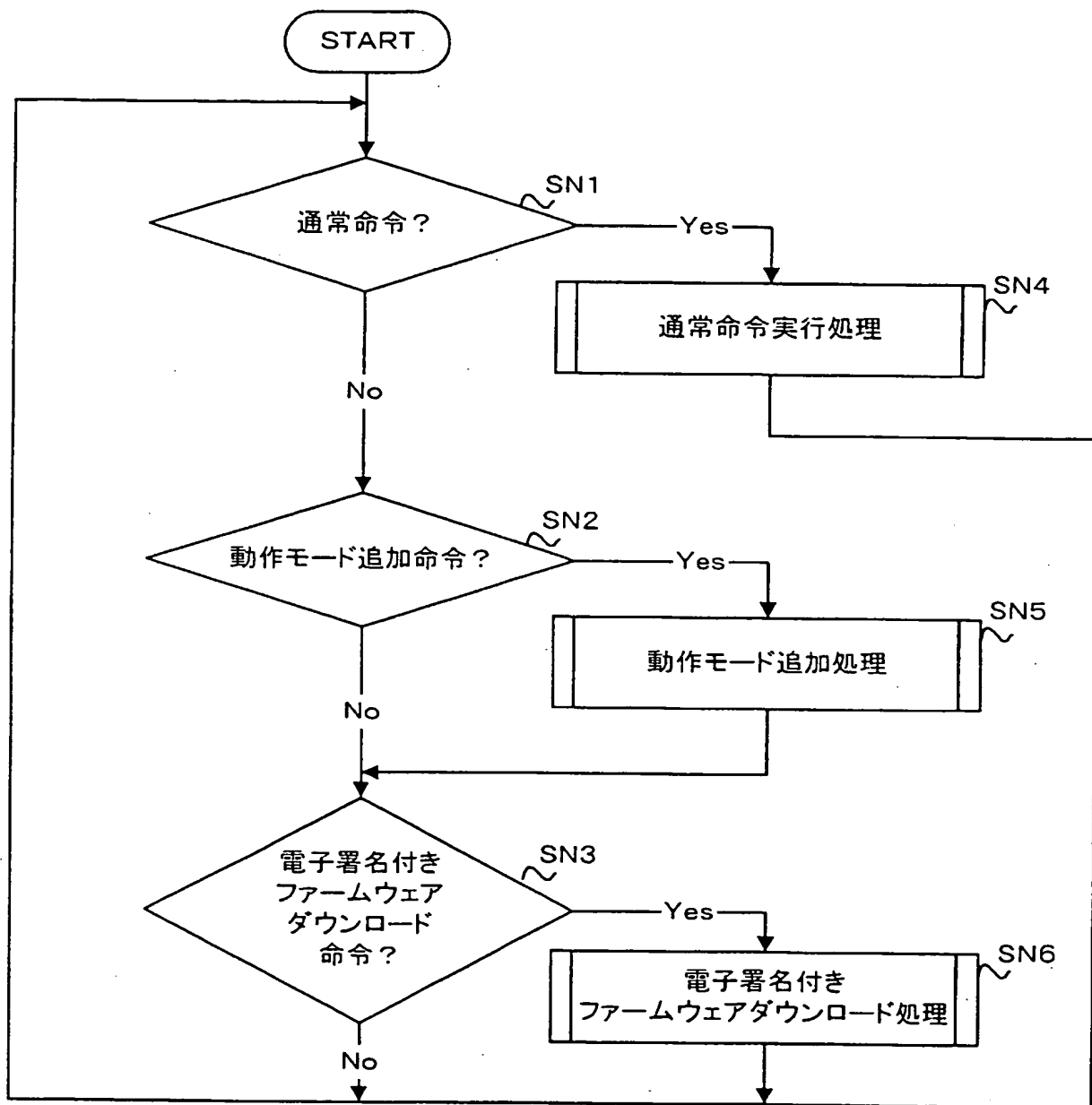
THIS PAGE BLANK (USPTO)

第22図



THIS PAGE BLANK (USPTO)

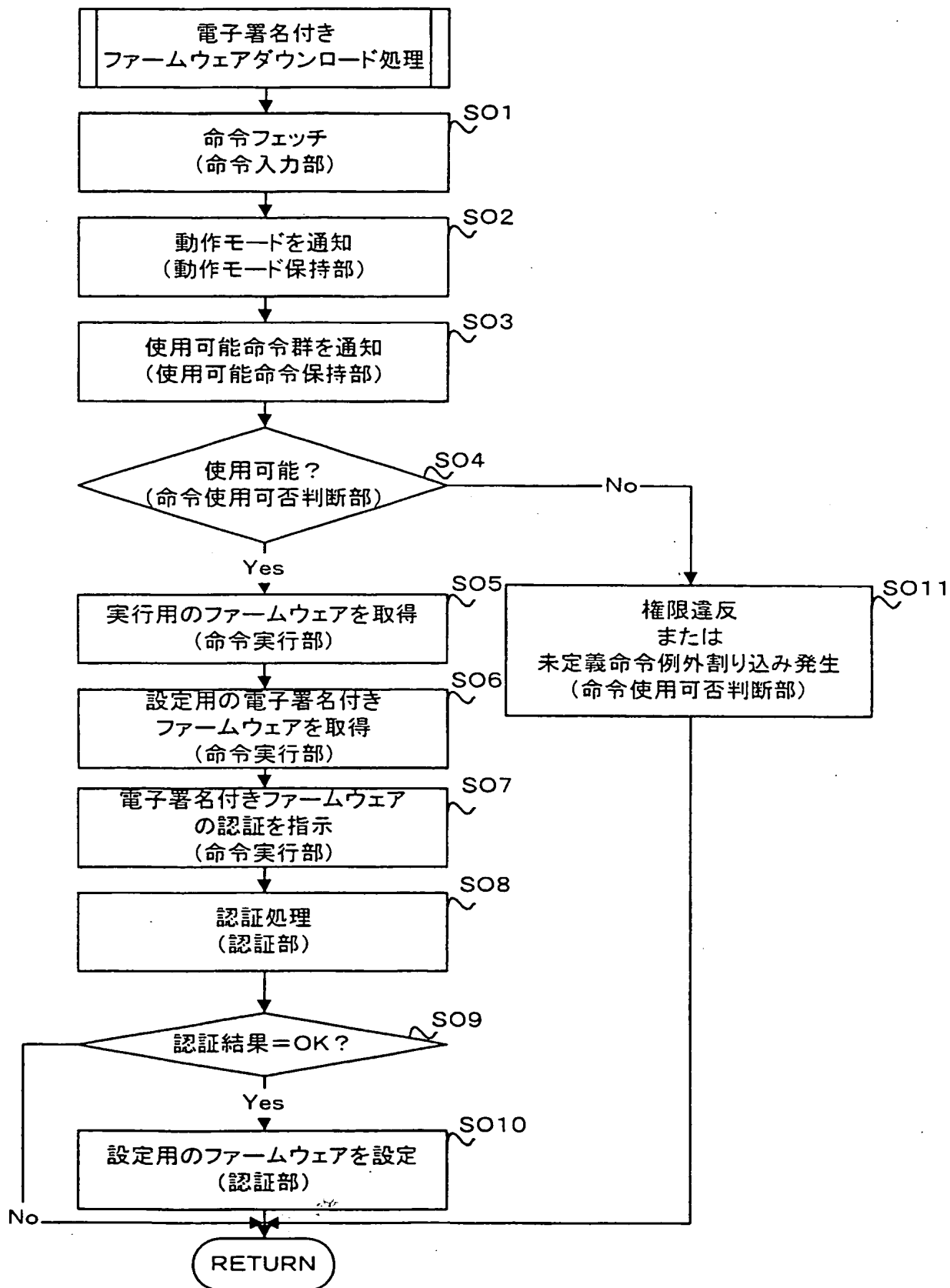
第23図



THIS PAGE BLANK (USPTO)

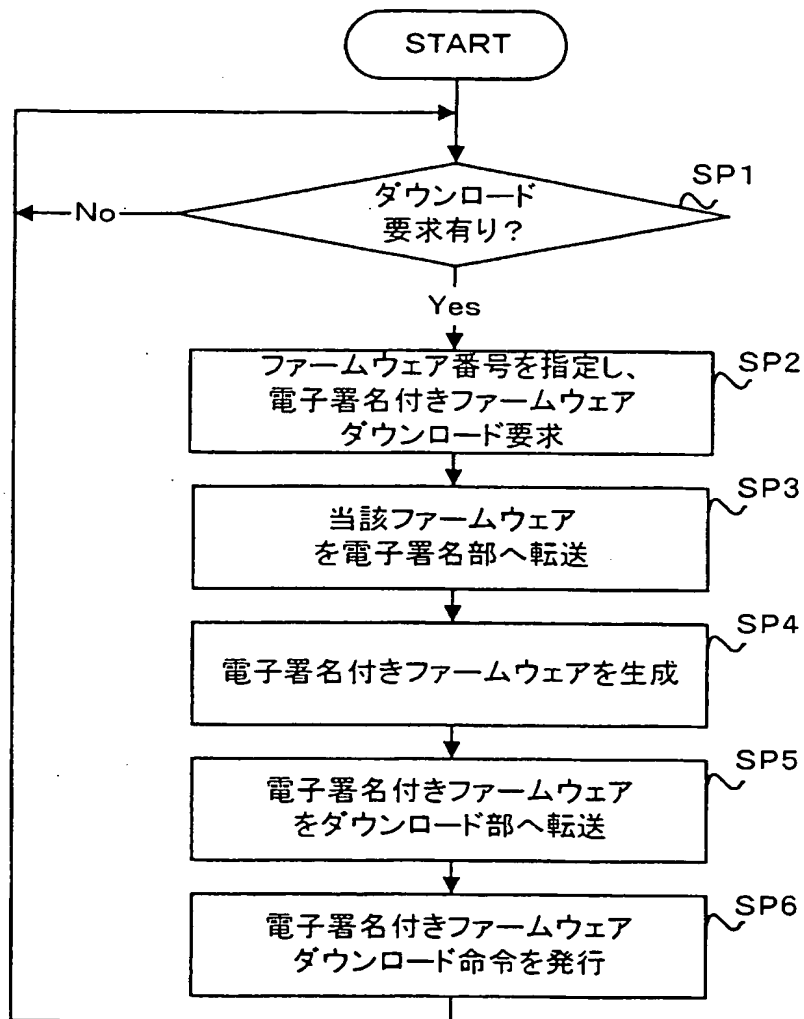
24/46

第24図



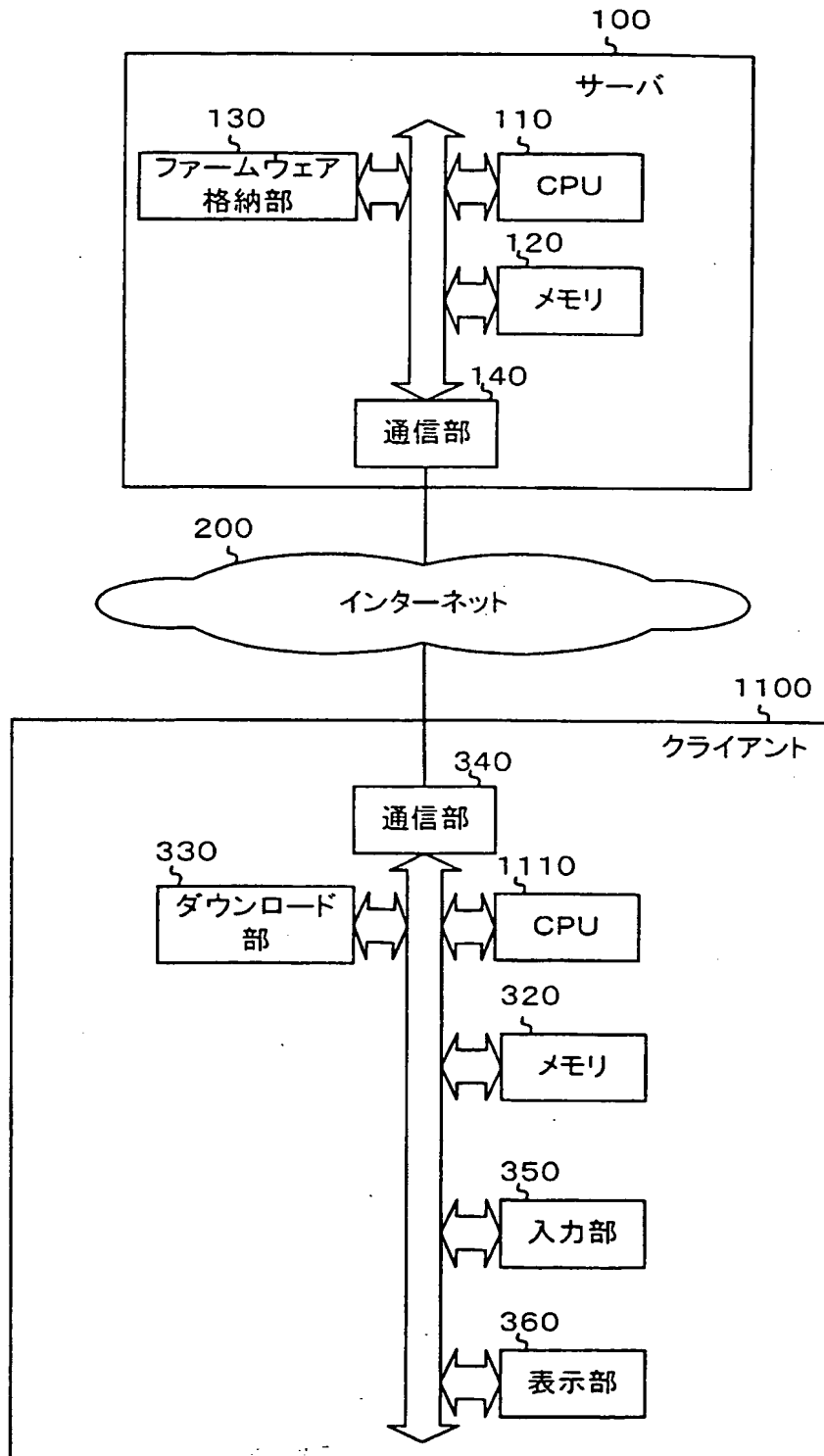
THIS PAGE BLANK (USPTO)

第25図



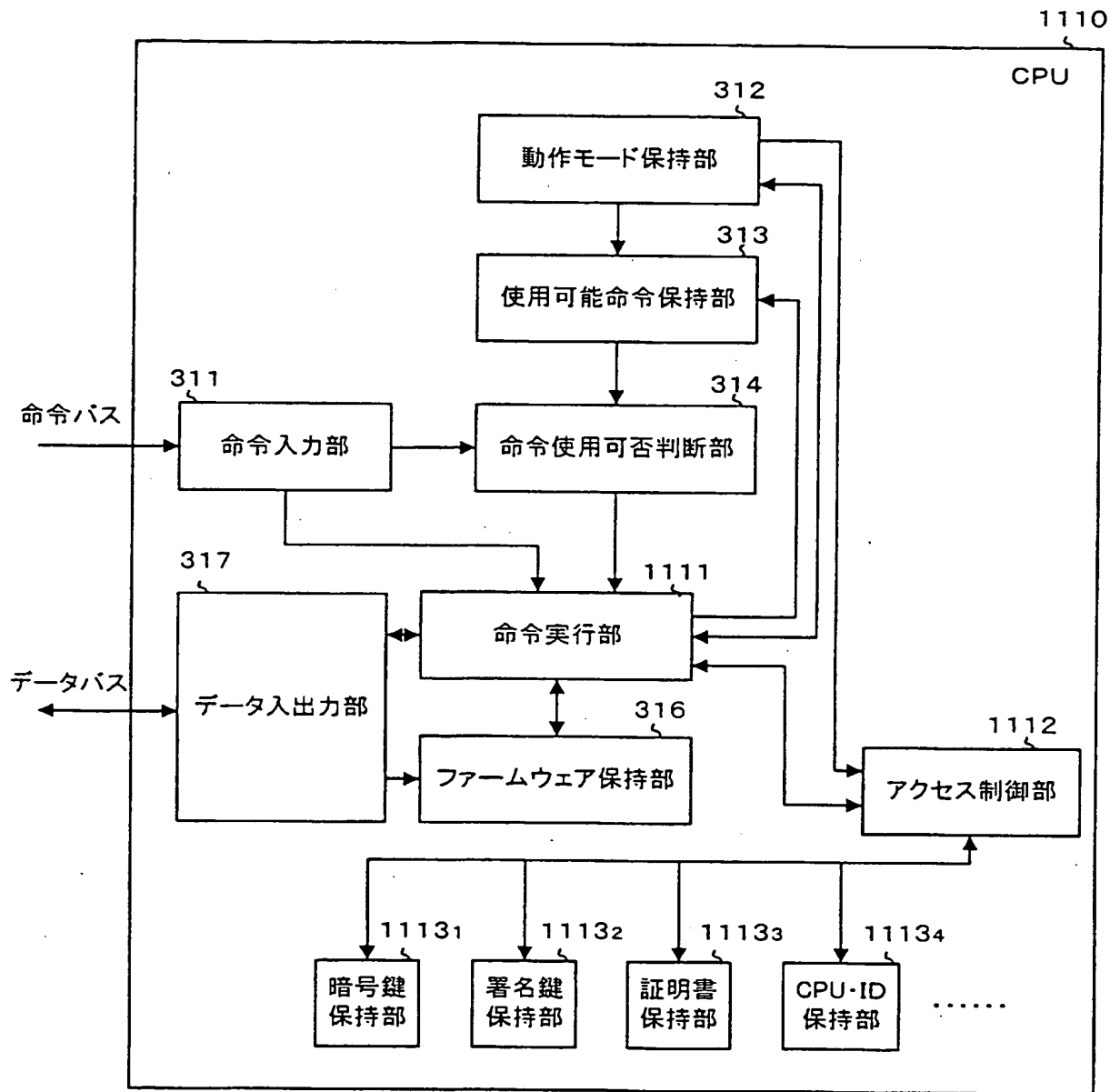
THIS PAGE BLANK (USPTO)

第26図



THIS PAGE BLANK (USPTO)

第27図



THIS PAGE BLANK (USPTO)

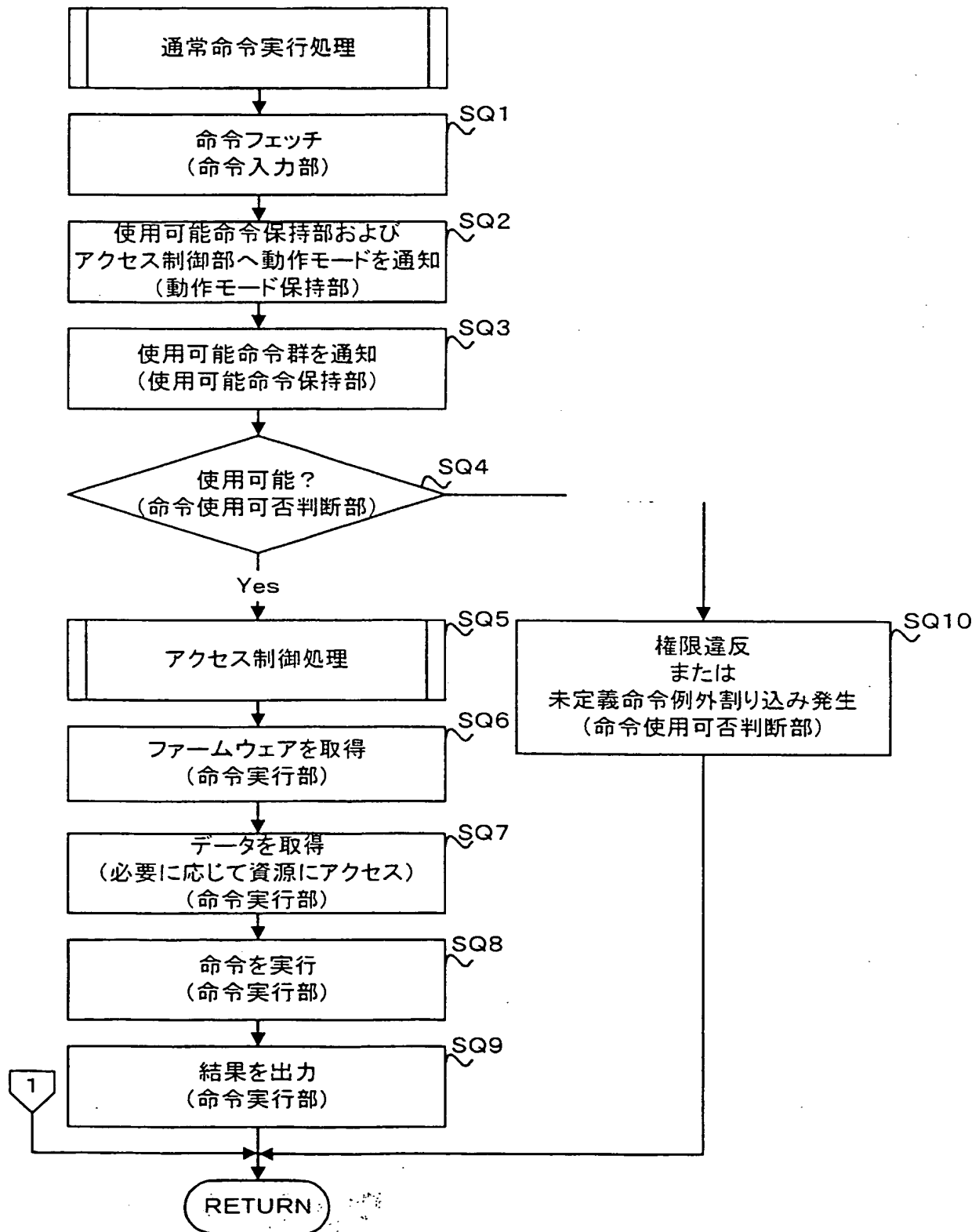
第28図

1200

動作モード	アクセス可能数	資源1	資源2	資源i	資源n
0	n	暗号鍵	署名鍵	証明書	CPU-ID
1	i	暗号鍵	署名鍵	CPU-ID	—	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
k	1	署名鍵	—	—	—	—	—

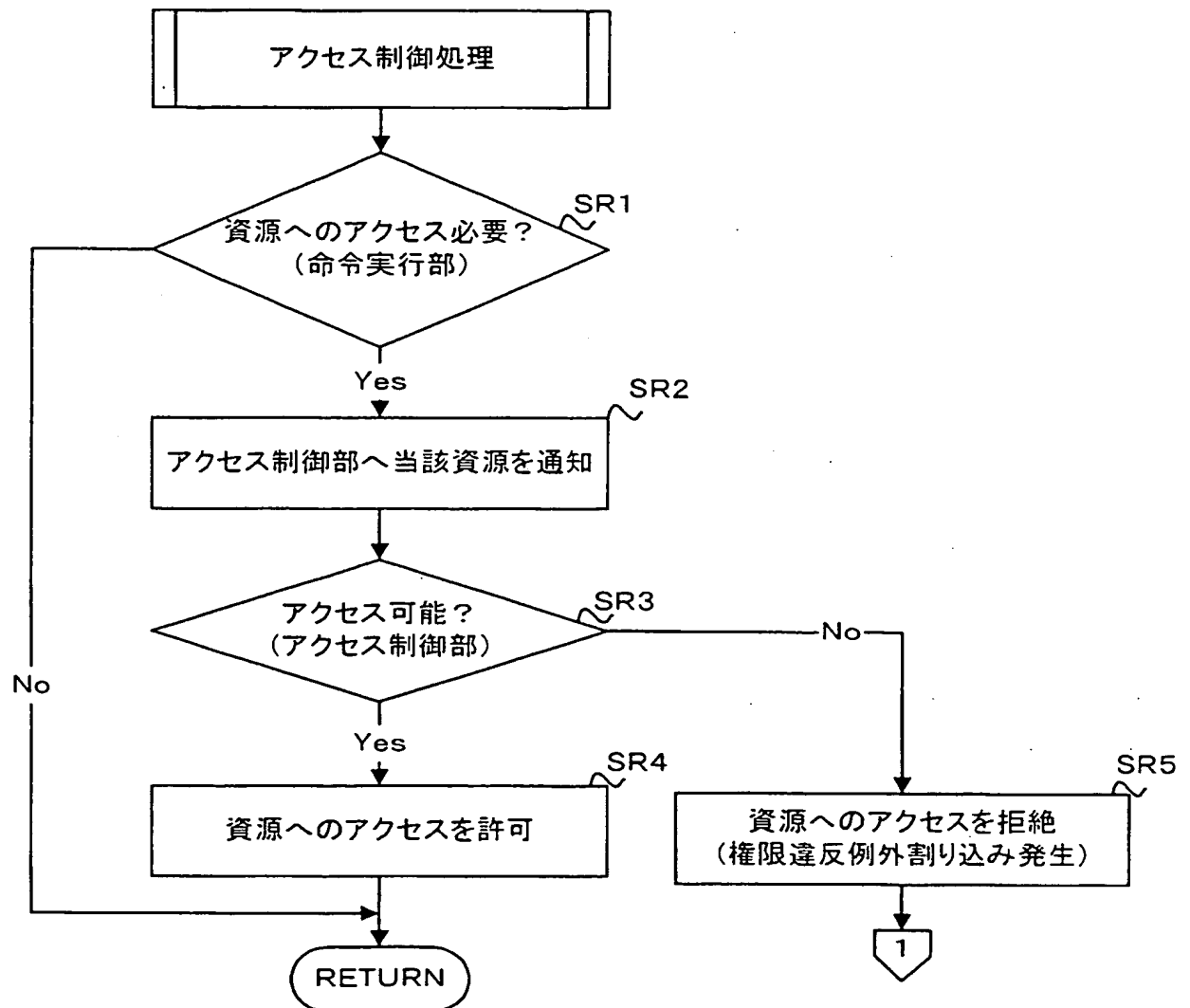
THIS PAGE BLANK (USPTO)

第29図



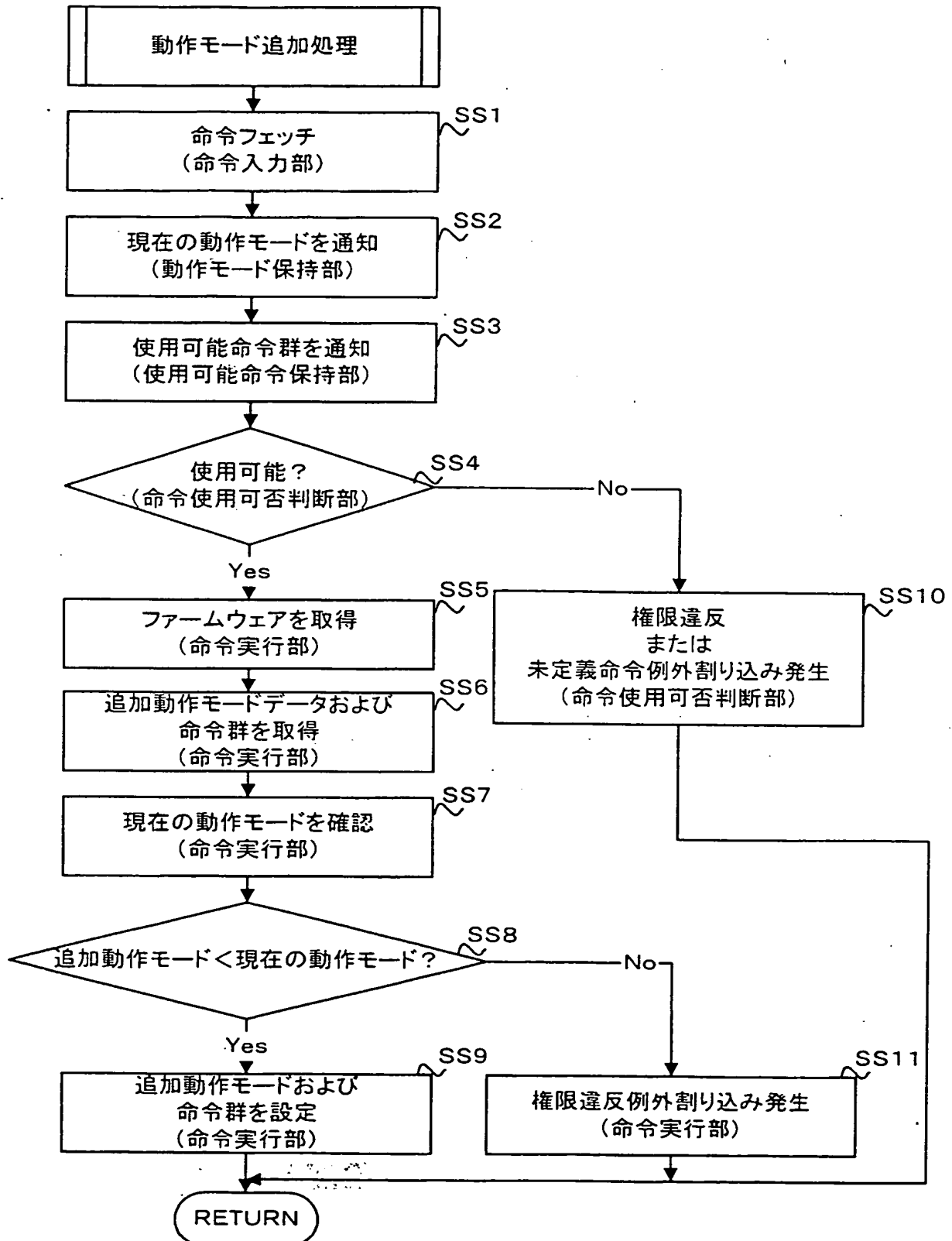
THIS PAGE BLANK (USPTO)

第30図



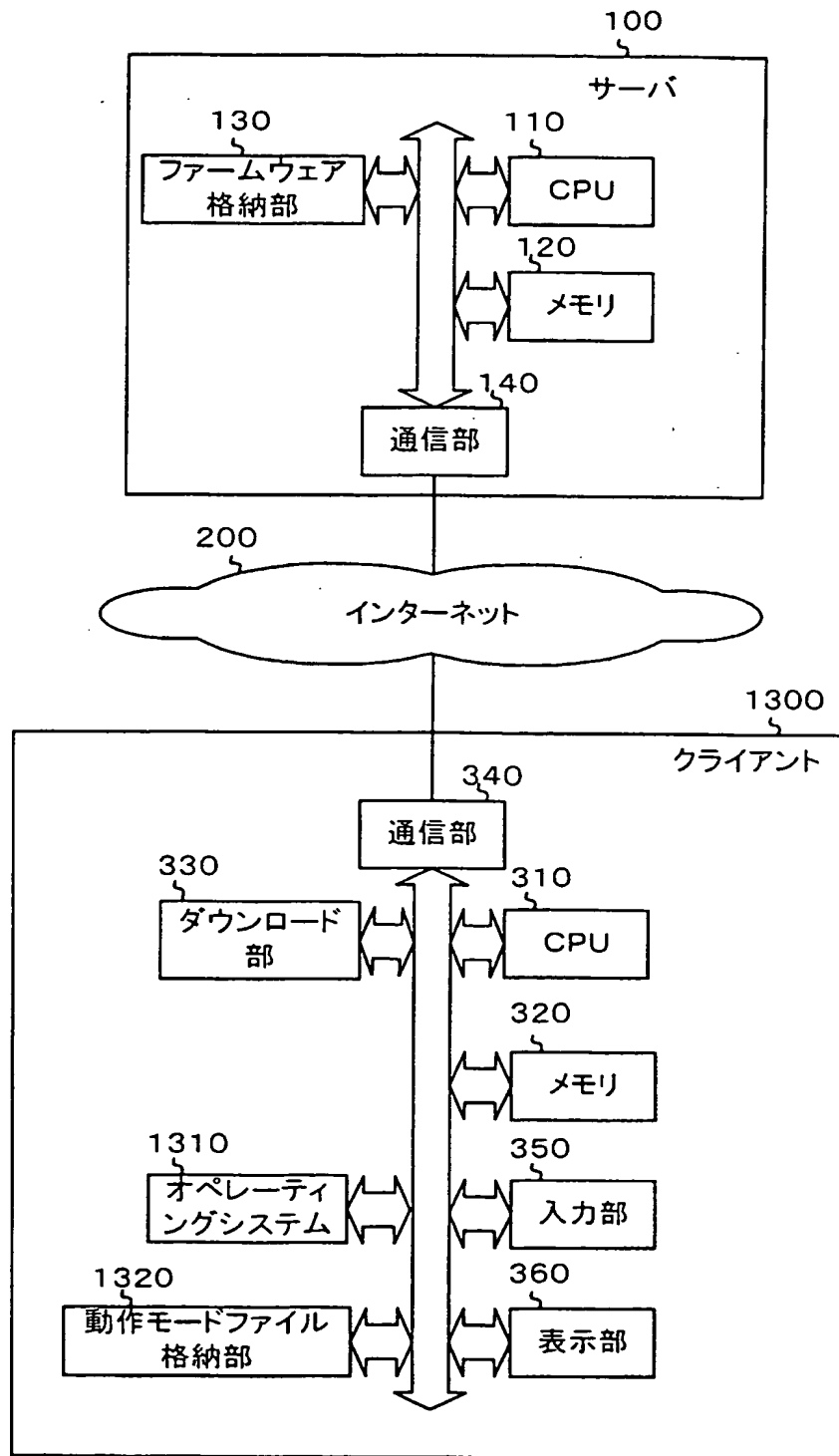
THIS PAGE BLANK (USPTO)

第31図



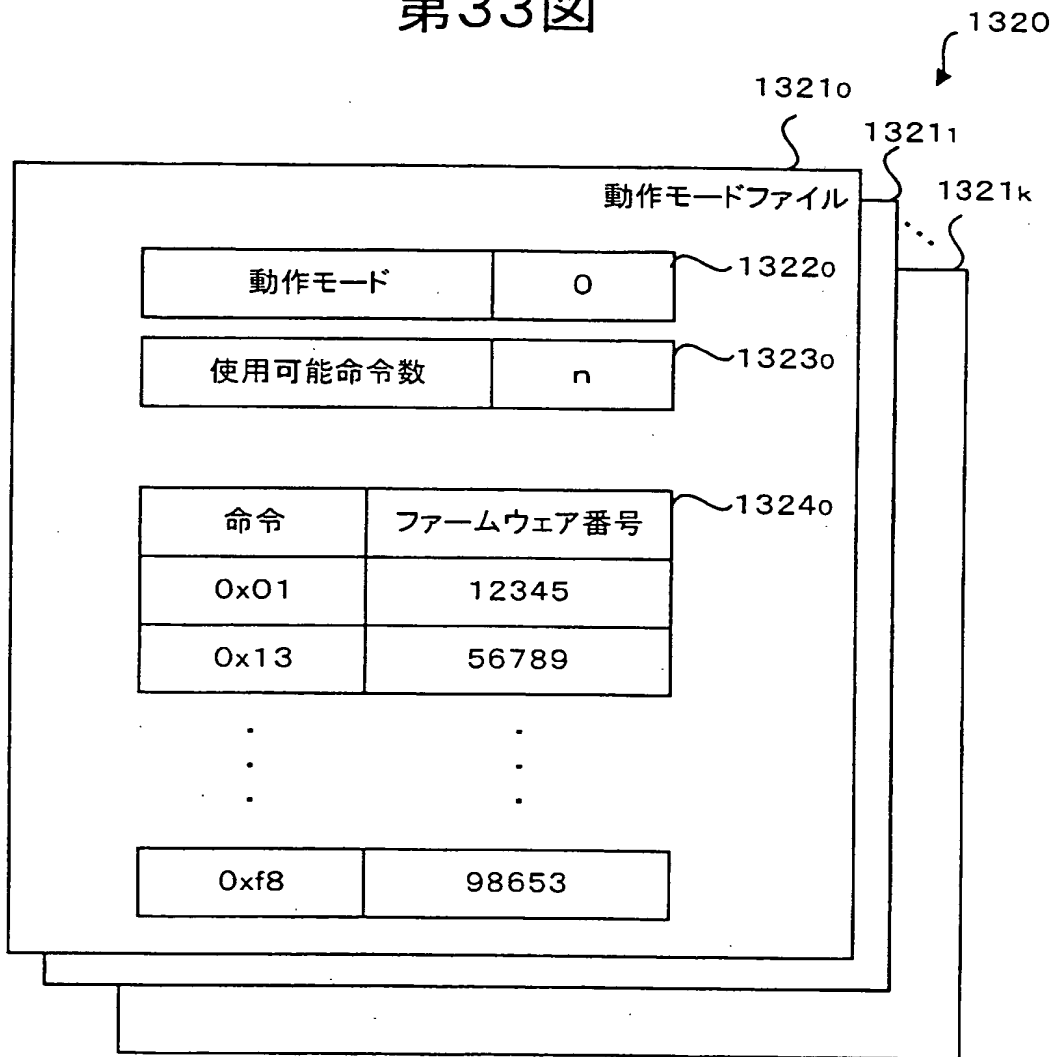
THIS PAGE BLANK (USPTO)

第32図



THIS PAGE BLANK (USPTO)

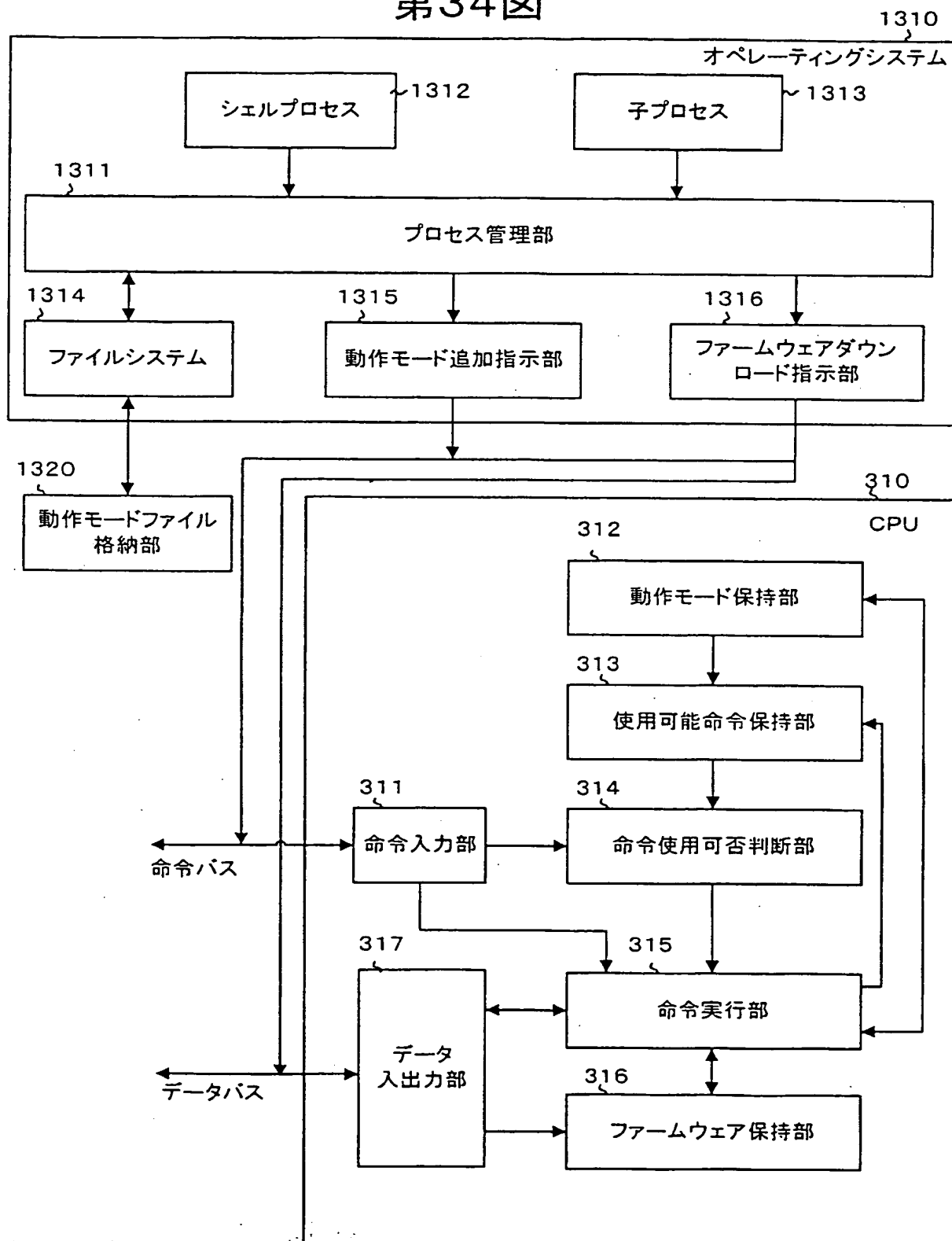
第33図



THIS PAGE BLANK (USPTO)

34/46

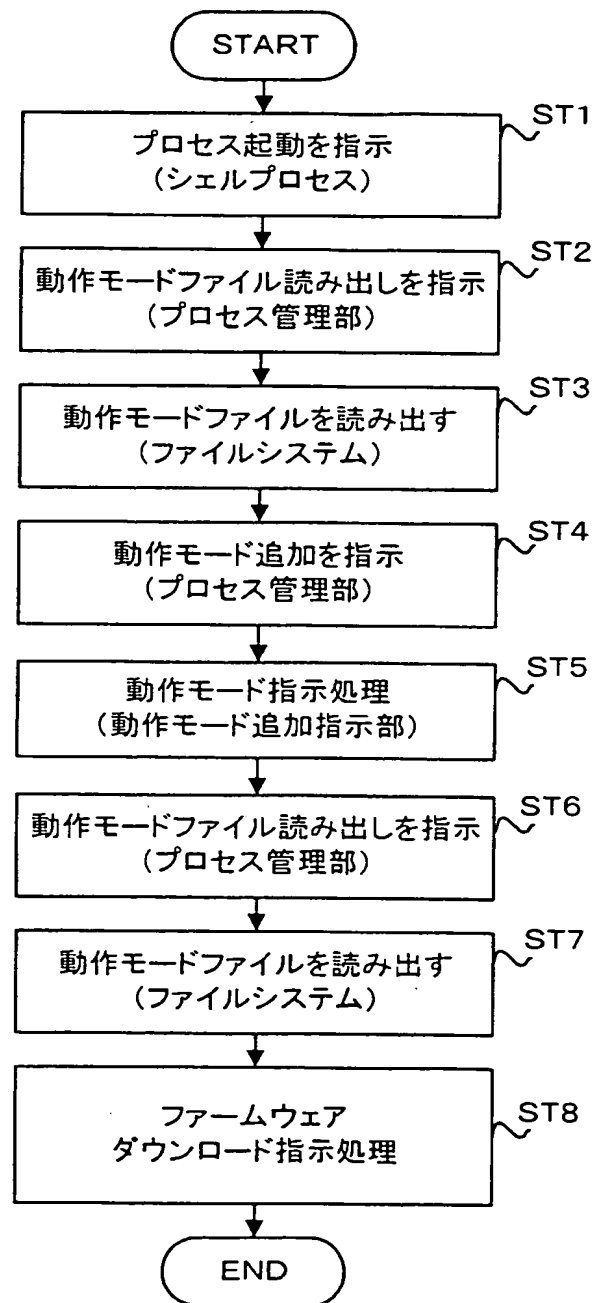
第34図



THIS PAGE BLANK (USPTO)

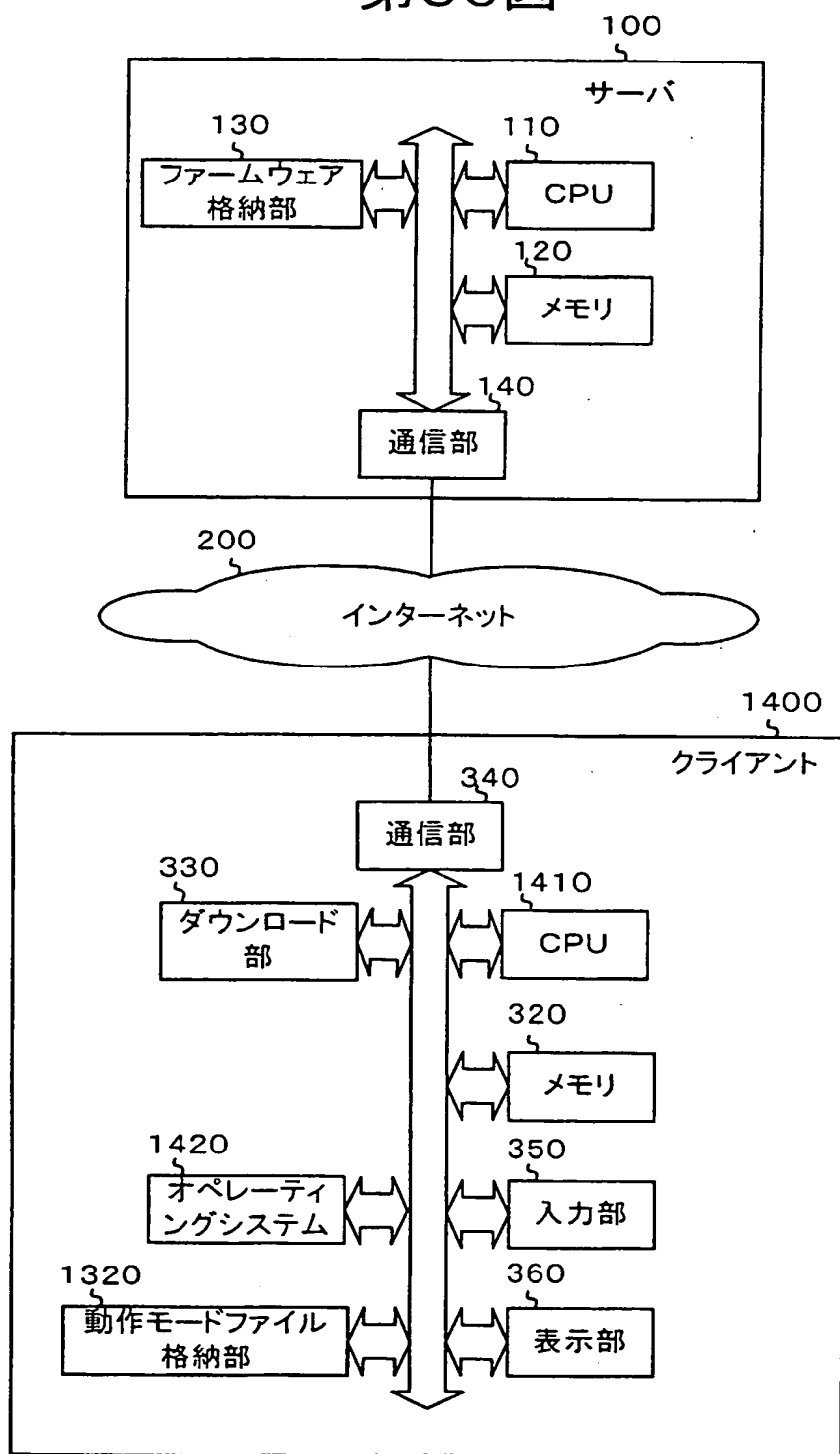
35/46

第35図



THIS PAGE BLANK (USPTO)

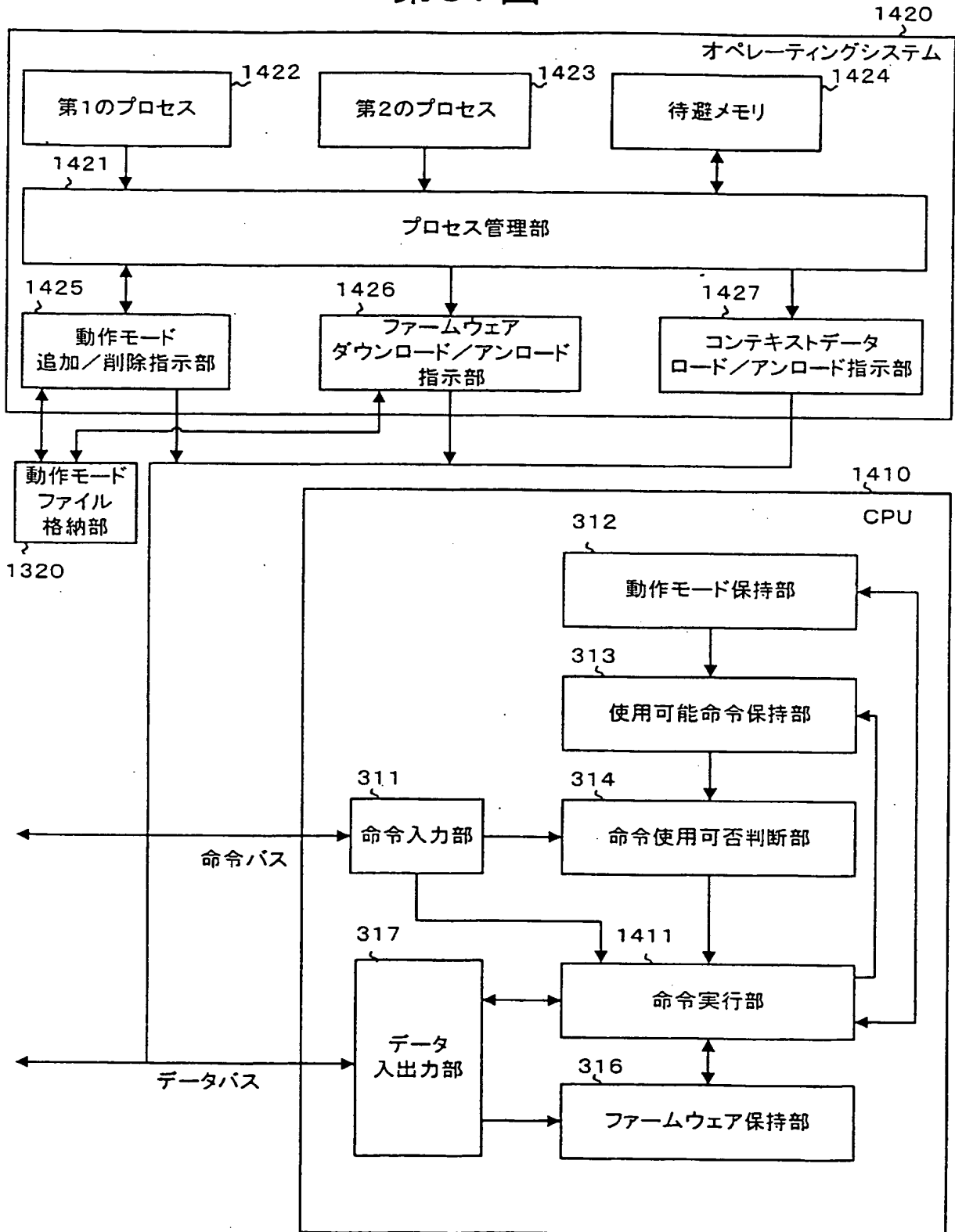
第36図



THIS PAGE BLANK (USPTO)

37/46

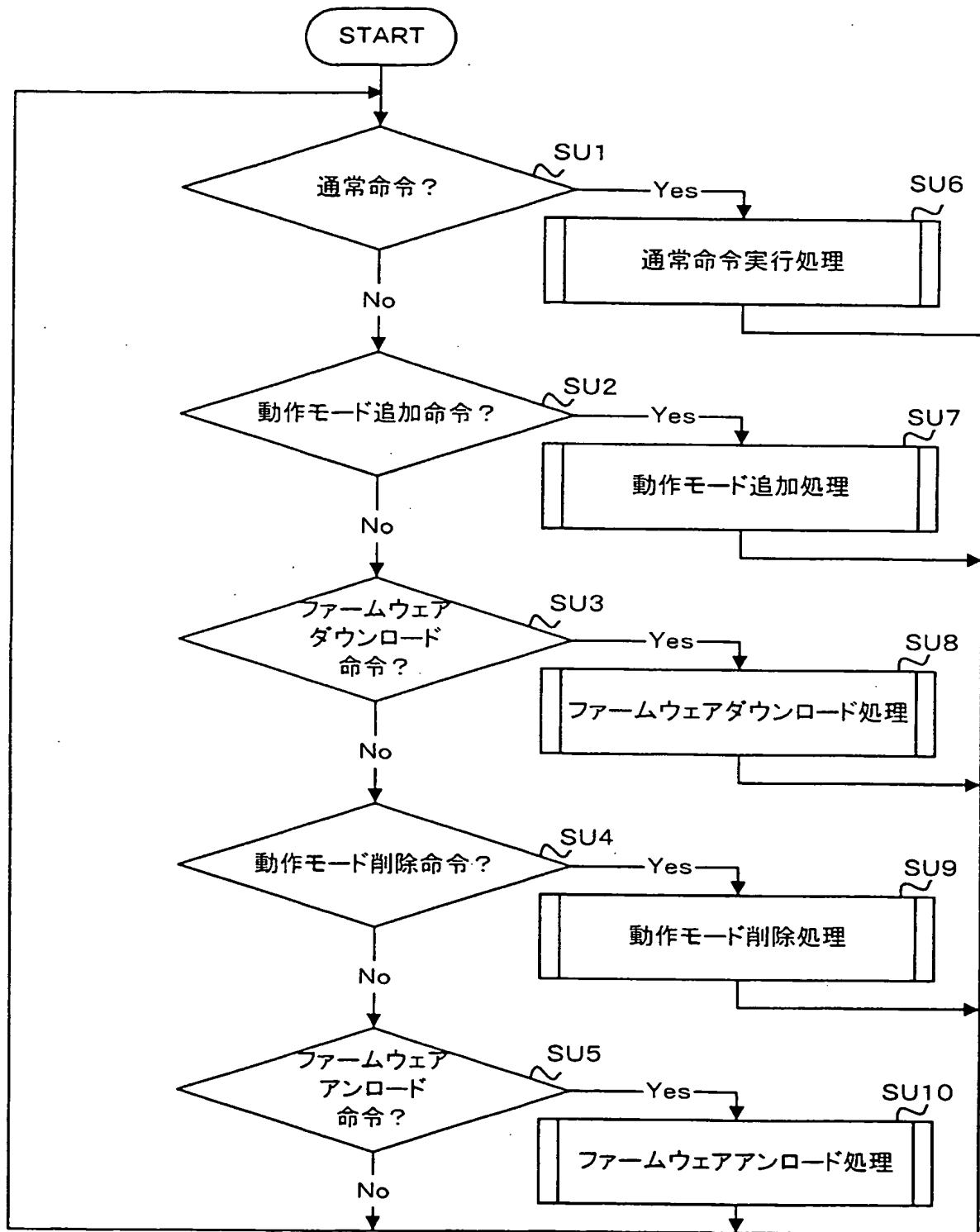
第37図



THIS PAGE BLANK (USPTO)

38/46

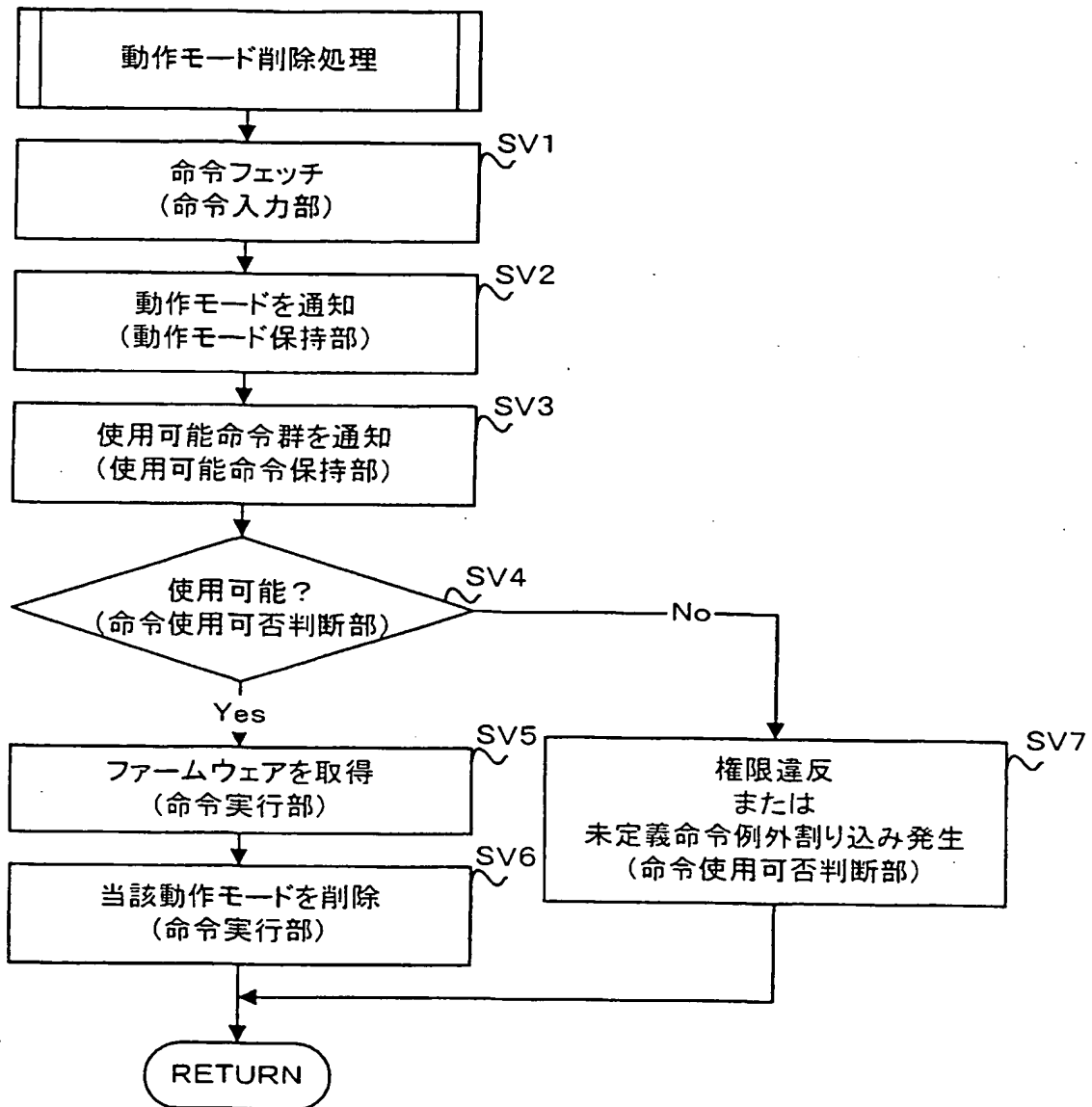
第38図



THIS PAGE BLANK (USPTO)

39/46

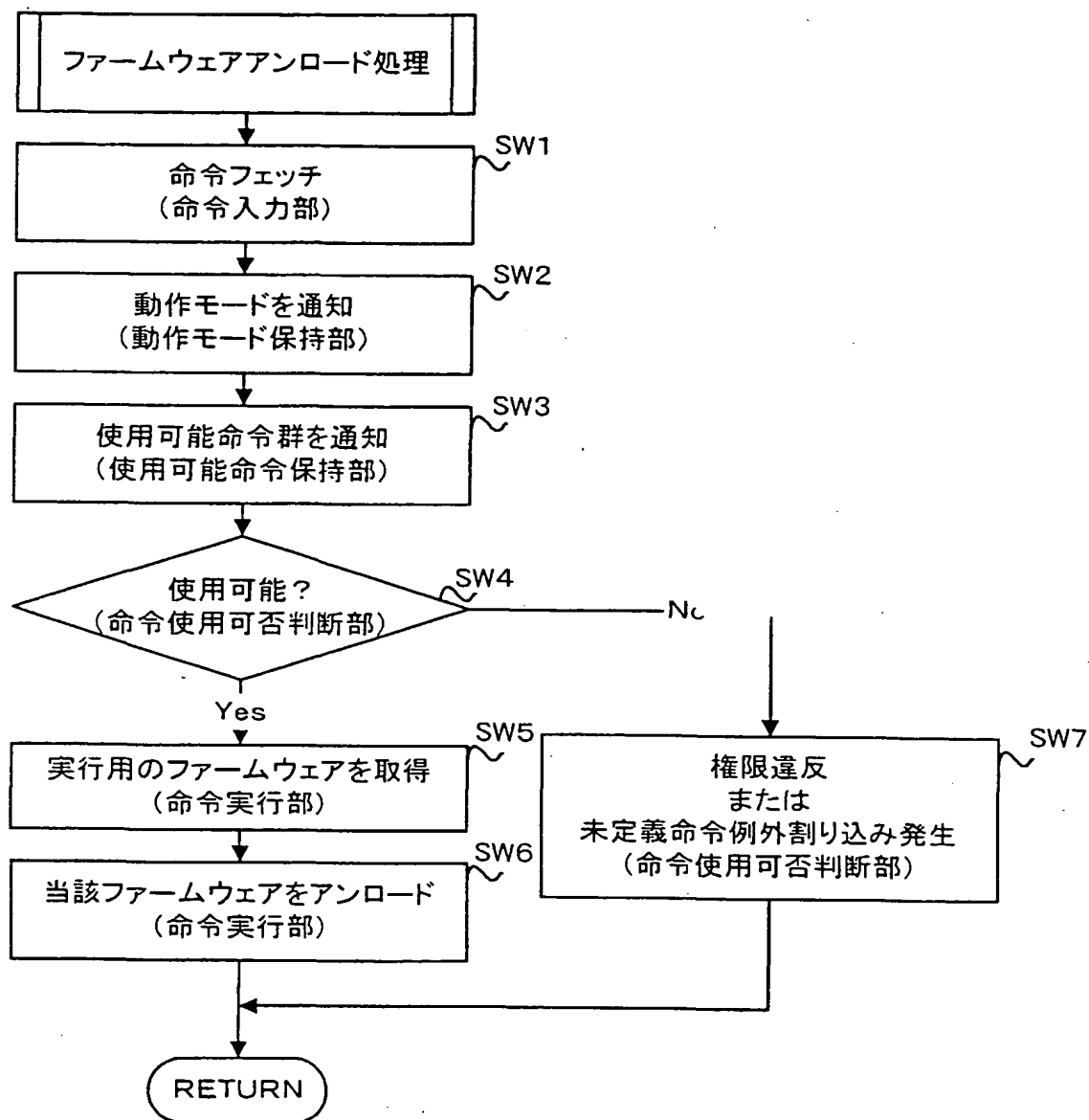
第39図



THIS PAGE BLANK (USPTO)

40/46

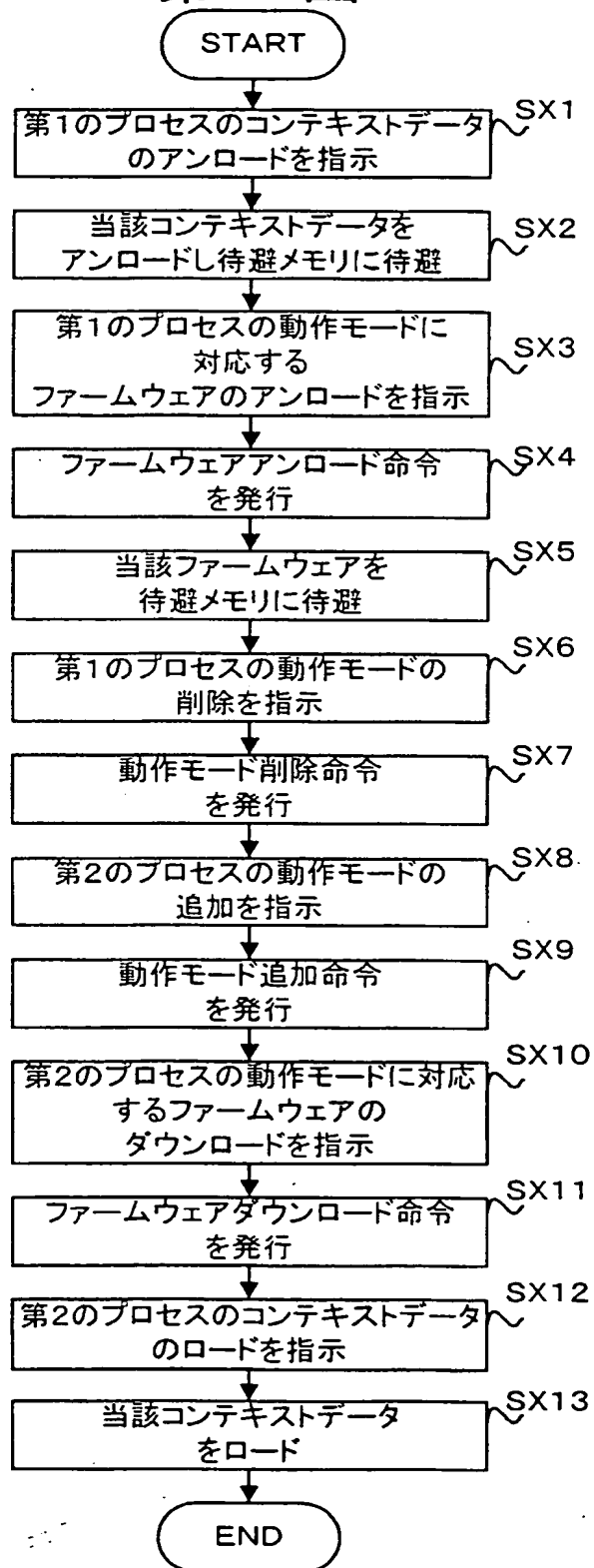
第40図



THIS PAGE BLANK (USPTO)

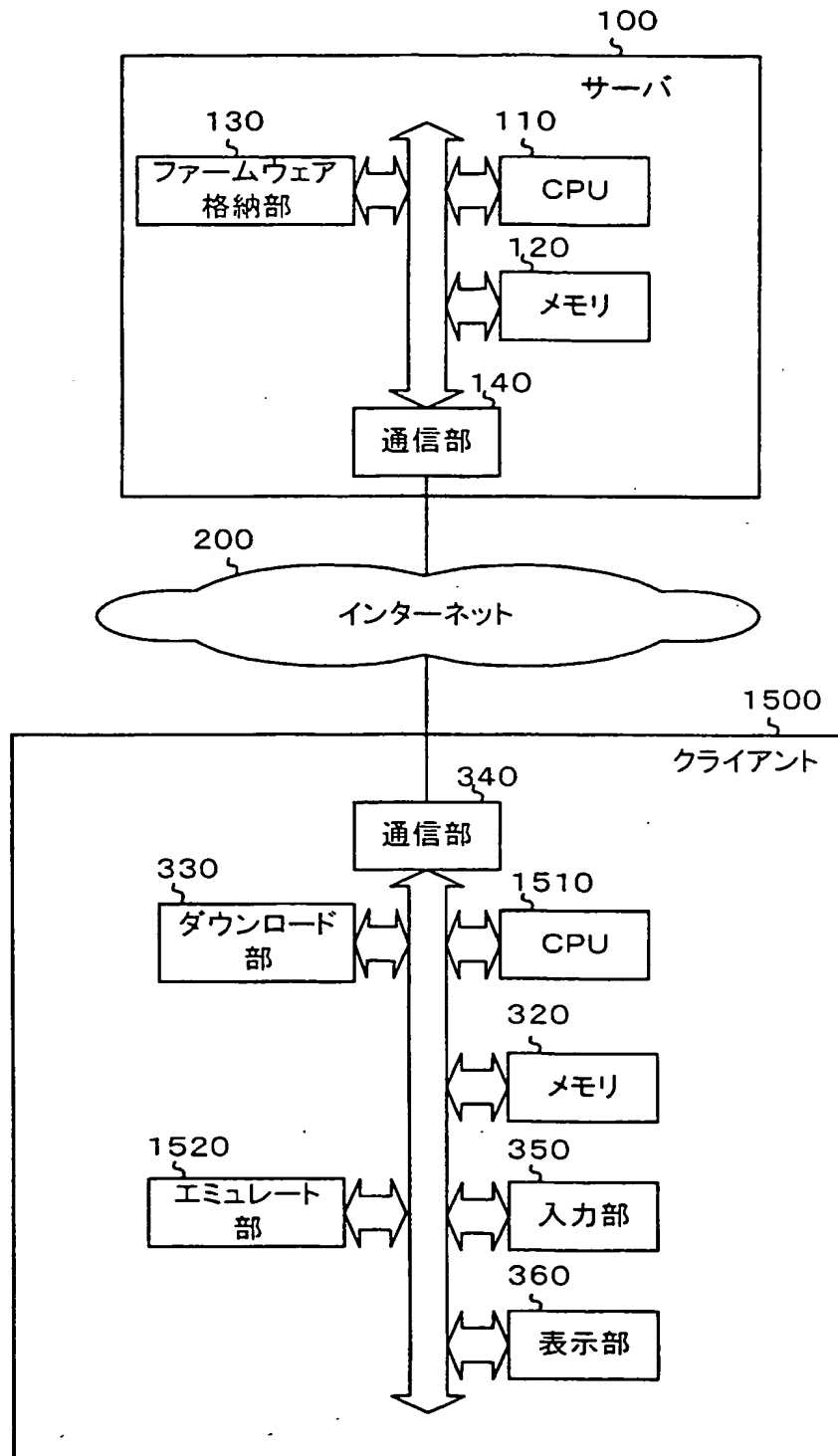
41/46

第41図



THIS PAGE BLANK (USPTO)

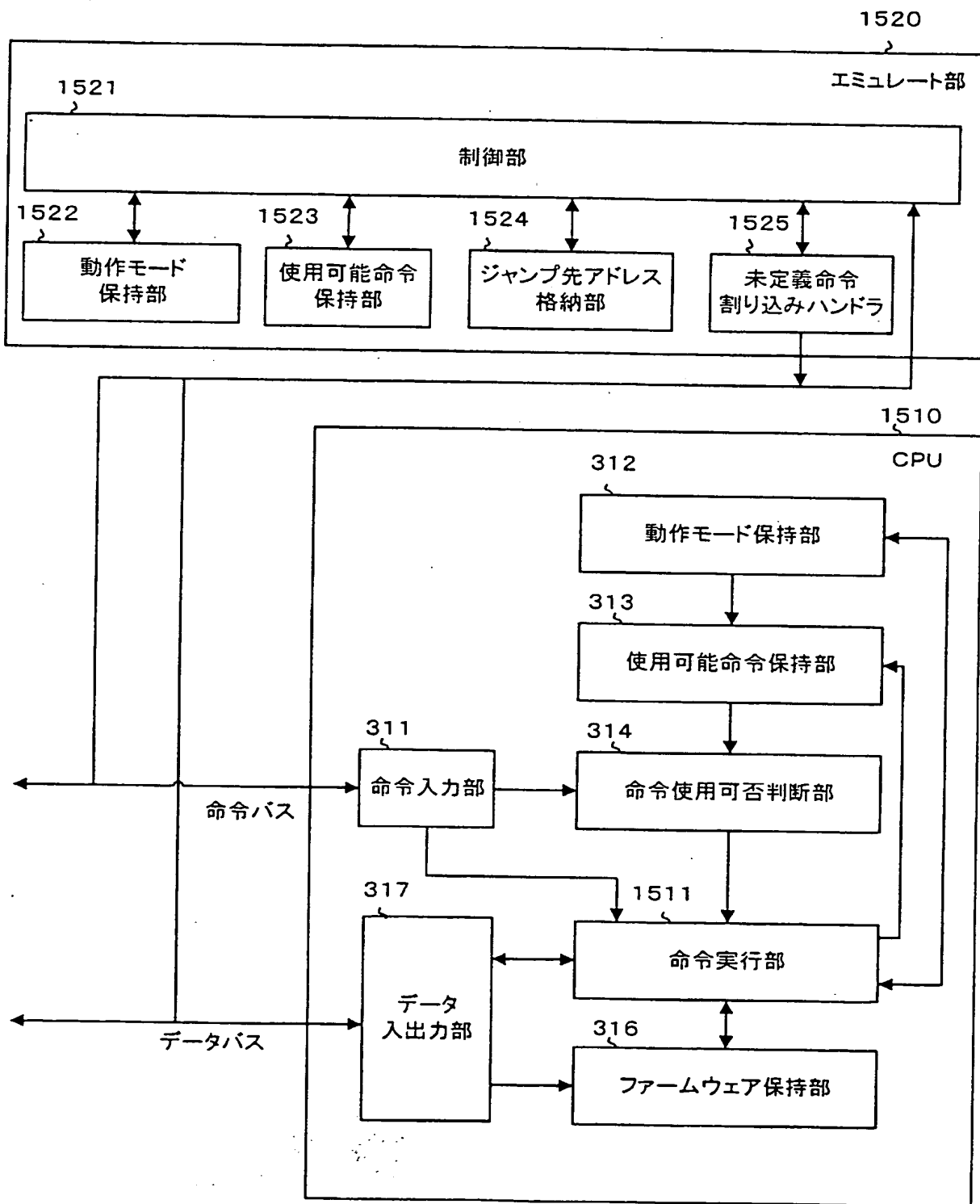
第42図



THIS PAGE BLANK (USPTO)

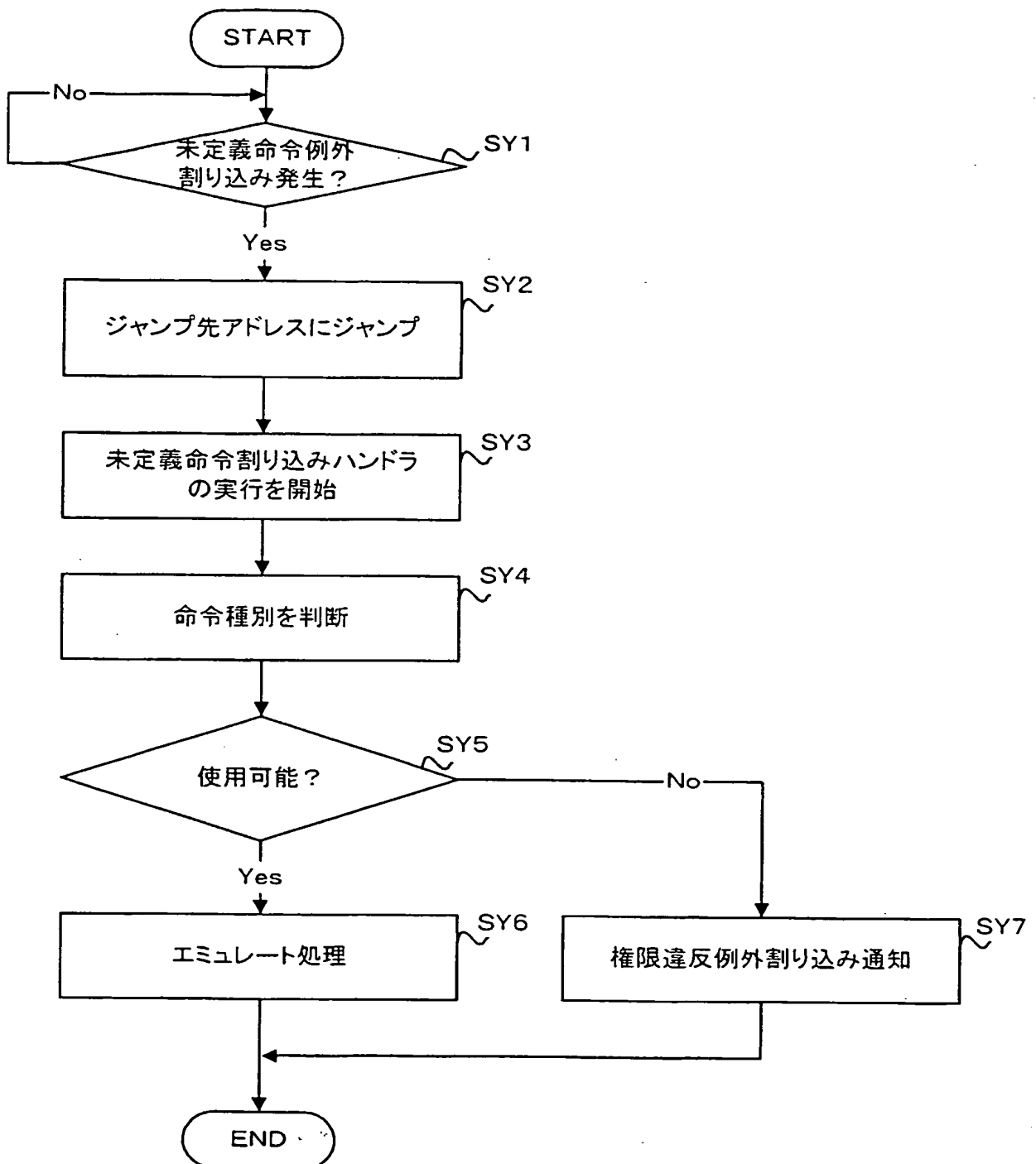
43/46

第43図



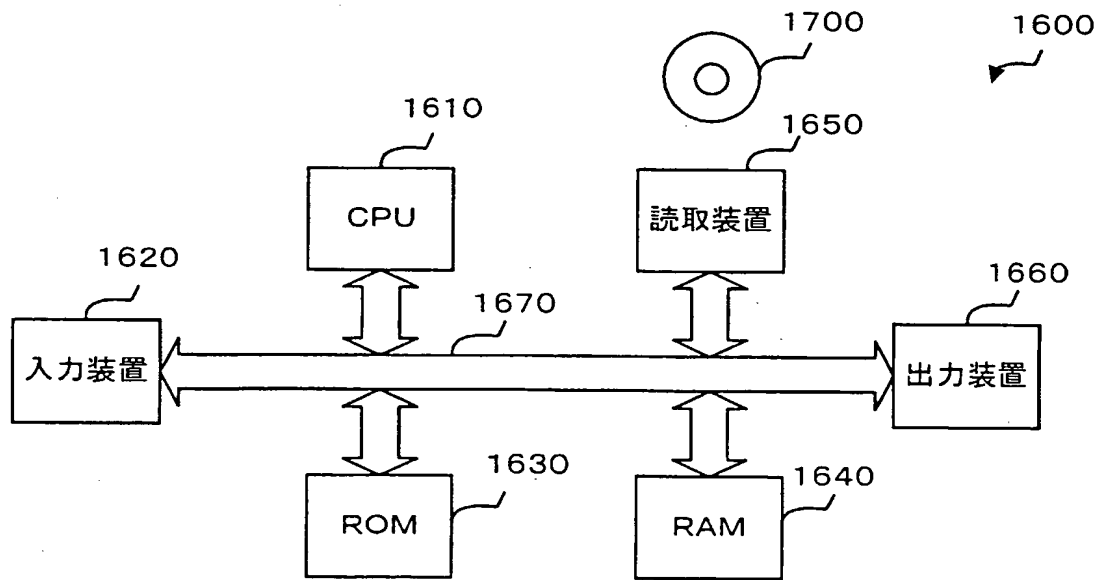
THIS PAGE BLANK (USPTO)

第44図



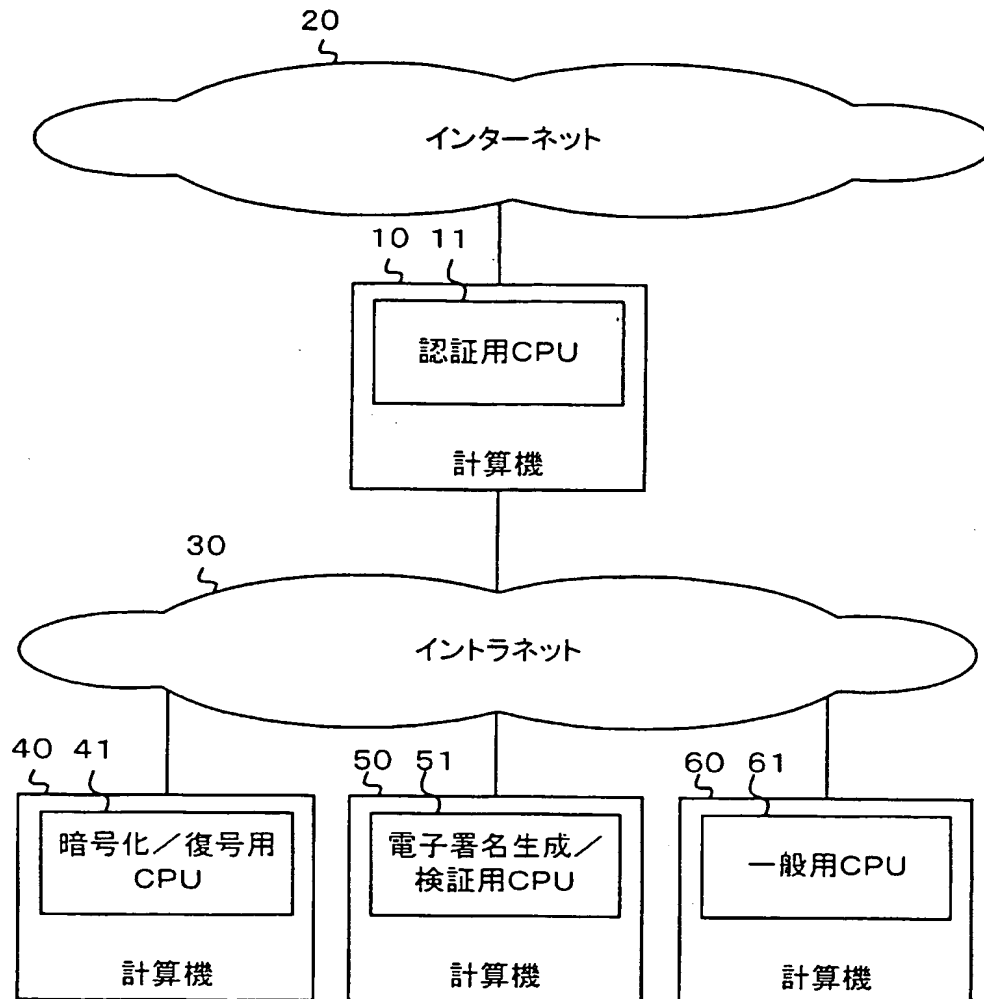
THIS PAGE BLANK (USPTO)

第45図



THIS PAGE BLANK (USPTO)

第46図



THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/10446

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F9/30, G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F9/30, G06F9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS), [DAUNRODO, FAMUEEA, RONRI KAIRO DETA, MAIKURO PUROGURAMU, MEIREI SETTO] (in Japanese)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 7-182155, A (Hitachi, Ltd.), 21 July, 1995 (21.07.95), Full text (Family: none)	1-10
A	JP, 2-231634, A (NEC Corp.), 13 September, 1990 (13.09.90), Full text (Family: none)	7
A	R.P.Bird, "A Dynamically Microprogrammable Machine as a Variable Function Resource in a Local Area Network", Systems Architecture, The International Computing Symposium, (1981), pages 37 to 45	1-10
A	Masataka KOTANI, Takashi MORIHARA, Naoya TORII, "Tokusyu: Kenkyu Kaihatsu Saizensen Internet Security", Fujitsu, Vol.52, No.4, (Fujitsu Ltd.), 13 July, 2001 (13.07.01), Pages 329 to 337	2, 3

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

12 March, 2002 (12.03.02)

Date of mailing of the international search report

19 March, 2002 (19.03.02)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl¹ G06F9/30, G06F9/06

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl¹ G06F9/30, G06F9/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2002年
 日本国登録実用新案公報 1994-2002年
 日本国実用新案登録公報 1996-2002年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS), [ダウンロード, ファームウェア, 論理回路データ, マイクロプログラム, 命令セット]

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 7-182155 A (株式会社日立製作所) 1995.07.21, 全文, (ファミリーなし)	1-10
A	JP 2-231634 A (日本電気株式会社) 1990.09.13, 全文, (ファミリーなし)	7
A	R.P.Bird, "A DYNAMICALLY MICROPROGRAMMABLE MACHINE AS A VARIABLE FUNCTION RESOURCE IN A LOCAL AREA NETWORK", SYSTEMS ARCHITECTURE, THE INTERNATIONAL COMPUTING SYMPOSIUM, (1981), pp. 37 - 45	1-10

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

12.03.02

国際調査報告の発送日

19.03.02

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号 100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

酒井 恭信

5B

9190

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	小谷誠剛, 森原隆, 鳥居直哉, “特集: 研究開発最前線 インターネットセキュリティ”, FUJITSU, VOL. 5 2, NO. 4, 富士通株式会社, (2001.07.13), pp. 329 - 337	2, 3